2010-09

Homeland security intelligence : to what end?

Miller, Andrew D.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOMELAND SECURITY INTELLIGENCE: TO WHAT END?

by

Andrew D. Miller

September 2010

Thesis Co-Advisors: Christopher Bellavita
Paul J. Smith

Approved for public release; distribution is unlimited

HIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Homeland Security Intelligence: To What End?		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Andrew D. Miller			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

In this thesis, I present potential solution sets to the question of why homeland security leaders and practitioners use intelligence to improve homeland security decisions. Specific roles and benefits of intelligence are identified, analyzed, and where applicable, extended to domestic security objectives across the homeland security community spectrum. This thesis purports and defends the theory that there are many and varied roles for intelligence for homeland security stakeholders. Six categories of benefits are presented as a frame work for homeland security decision makers, especially those with limited prior knowledge of threat intelligence, to consider as they conceptualize the employment or expectations of intelligence in a homeland security context. The adaptive threat orientation is introduced as a model for acquisition and maintenance of persistent decision advantage in the homeland security threat-scape.

The adaptive threat orientation model relies on a continual, repeatable and consistent process, whereby homeland security leaders can acquire and maintain decision advantage over an adversary in the homeland security decision space. This thesis defines homeland security decision advantage, the elements necessary for its acquisition and maintenance, and ultimately defines and defends the value of intelligence in improving homeland security decisions.

14. SUBJECT TERMS adaptive threat orientation, homeland security, homeland security intelligence, intelligence, intelligence theory, decision making, decision science, domestic intelligence, threat awareness, decision advantage, Washington State Air National Guard			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HOMELAND SECURITY INTELLIGENCE: TO WHAT END?

Andrew D. Miller
Captain, Esq., Washington State Air National Guard
B.S., Excelsior College, 2000
M.A., Organizational Leadership, Gonzaga University, 2004
J.D., Seattle University School of Law, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Andrew D. Miller

Approved by: Christopher Bellavita
Thesis Co-Advisor

Paul Smith
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, I present potential solution sets to the question of why homeland security leaders and practitioners use intelligence to improve homeland security decisions. Specific roles and benefits of intelligence are identified, analyzed, and where applicable, extended to domestic security objectives across the homeland security community spectrum. This thesis purports and defends the theory that there are many and varied roles for intelligence for homeland security stakeholders. Six categories of benefits are presented as a frame work for homeland security decision makers, especially those with limited prior knowledge of threat intelligence, to consider as they conceptualize the employment or expectations of intelligence in a homeland security context. The adaptive threat orientation is introduced as a model for acquisition and maintenance of persistent decision advantage in the homeland security threat-scape.

The adaptive threat orientation model relies on a continual, repeatable and consistent process, whereby homeland security leaders can acquire and maintain decision advantage over an adversary in the homeland security decision space. This thesis defines homeland security decision advantage, the elements necessary for its acquisition and maintenance, and ultimately defines and defends the value of intelligence in improving homeland security decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	September 11, 2001
CIA	Central Intelligence Agency
CHDS	Center for Homeland Defense and Security
DHS	Department of Homeland Security
DoD	Department of Defense
DoJ	Department of Justice
FBI	Federal Bureau of Investigations
HAS	Homeland Security Act
HSINT	Homeland Security Intelligence
HSOC	Homeland Security Operations Center
I&A	Information and Analysis
ITACG	Interagency Threat Assessment Coordination Group
FEMA	Federal Emergency Management Agency
NCTC	National Counter-terrorism Center
NSB	National Security Branch
OODA	Observe-Orient-Decide-Act
ODNI	Office of the Director of National Intelligence
U.S.C.	United States Code
U.S.	United States
USA	United States Army
USIC	United States Intelligence Community

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

> *Understanding how to act under conditions of incomplete information is the highest and most urgent human pursuit.*
>
> Nassim Nicholas Taleb (2007, p. 57)

This thesis is not about how to "fix" or to intentionally aggrandize the role of intelligence in homeland security. My objective here is to 1) identify and demonstrate the many and varied roles and benefits that intelligence may play in supporting the acquisition and maintenance of decision advantage in the homeland security threat-scape, and 2) potentially revolutionize the manner in which those decisions are made and dramatically increase the collective benefit of optimized homeland security policy and resource decisions to the nation by better understanding the role and benefits of using intelligence in homeland security.

A career intelligence officer, the first time I had to justify what I do was when I became a student at the Center for Homeland Defense and Security (CHDS) at the Naval Postgraduate School. An eclectic master's degree program that brings together homeland security leaders and practitioners from across the country and across the homeland security enterprise, the CHDS experience prides itself (and rightly so) as challenging its students to critically analyze most every aspect of homeland security in both sum and parts. When asked by a classmate, a fire chief from a major metropolitan city that had firsthand experience in responding to an act of devastating domestic terrorism, "Andrew, where were you guys (the intelligence community) on that one?," the best I could come up with was the well rehearsed "We have to be right every time, the terrorists only have to be right once." Another classmate, a career public health officer responded, "I've gone my entire career without using intel, and, frankly, I don't see what all the fuss is about." After discussing my thoughts on "fixing" some of the procedural issues related to intelligence another colleague dead panned, "So you 'fix' the intel community, so what? **What you do doesn't matter until it changes what I do**. [emphasis added]" Bingo. Those words "What you do doesn't matter until it changes what I do" would drive almost every facet of research for this project. I picked apart every word of that sentence in an

effort to understand better what "change" meant, what it means to "matter," who else "I" represented, and probably most important, the "whats" of homeland security that could be improved by the greater threat understanding only intelligence could provide. This thesis is my version of the "so what" to why homeland security leaders and practitioners may be well served to more closely examine the role, purpose, and value of intelligence within their decision-making processes. Intelligence is not, should not, and cannot be an end unto itself (Keegan 2004, p. 321). In order to be of any actual value, it must serve an end, and in the case of homeland security, that end ought to be a risk-based tactical, operational, political, or legal **judgment**. As such, I suggest the ***purpose*** of homeland security intelligence is not to acquire threat data, or draft reports or predict adversary activity; rather, the *purpose* of homeland security intelligence should be to **facilitate decision advantage** for leaders and practitioners within the homeland security strategic, operational, or tactical decision-making environments. Intelligence only becomes "value-added" for homeland security decision makers when the potential or anticipated benefits of using intelligence outweigh the costs or potential consequences of not using intelligence in support of decision processes. I believe an incredible and virtually untapped value and opportunity exists for homeland security and intelligence community leaders and practitioners willing and able to take a hard look at how a tailored, timely, and accurate threat orientation might change the face, and ultimately the outcomes sought within the homeland security environment.

A familiar maxim in the marketing industry is half of all marketing costs are wasted—but one can never be sure of which half (Neff, 2010). Similarly, with intelligence, the value of intelligence can go largely unrecognized until the consequences of ignoring or misunderstanding threats lead to decisions being made in ignorance to or without regard to available threat information that can lead to catastrophic **security** (not intelligence) failures.

I propose homeland security decision makers operating within a complex and dynamic threatscapewhom have acquired an appreciation for the role, purpose, and value (usefulness) of intelligence and have a realistic expectation of the derived benefits of homeland security intelligence will find themselves better able to leverage that

understanding in their decision making favor, potentially contributing to more effective, efficient, and persistent security decision advantage in comparison to those or against those lacking such an understanding.

This thesis is organized into three sections:

- The Role of Intelligence in Homeland Security
- How Homeland Security Decision Advantage can be Acquired and Maintained
- Six Derived Benefits of Intelligence-Based Homeland Decision Advantage

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It may take a village to raise a child, but in true homeland security fashion, it takes a multi-agency, joint coalition of collaborative, high-performing, over-achieving, and tireless family members, scholars, practitioners, and friends to write a thesis. My first and best love and appreciation go to my wife, Holly, and our six children for enduring well the time and attention diverted to this project. Very special thanks to my advisors and mentors Chris Bellavita and Paul Smith, and the entire staff and faculty at the Center for Homeland Defense and Security. Additionally, I owe a significant measure of gratitude to Major Generals Timothy Lowenberg and Gary Magonigle and Colonel Jerry Kosierowski for their vision, leadership, and thoughtful mentorship, as well as their invitation to embrace the complex and dynamic challenges of homeland security and contribute where and when I can, to the greatest extent of my talents and abilities.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> *How can any man say what he should do himself if he is ignorant about what his adversary is about?*
>
> Baron Antoine-Henri Jomini (as quoted by Rosello, 1991, p. 109)

A. PROBLEM STATEMENT

The role and derived benefits of intelligence in acquiring and maintaining homeland security decision advantage is insufficiently understood, valued or utilized in pursuit of strategic, operational, and tactical homeland security objectives.

The American homeland security threatscape is neither a private sector, federal, state, nor local domain, it is a *national* domain wherein threats of violence and security activities (homeland security efforts) are in constant, and usually, counterbalancing movement (Department of Homeland Security [DHS], 2007, p. 1). The specific value of intelligence within this arena has never been evaluated or subjected to any serious scrutiny—it is as if the intelligence community sees its value as self-evident while the academic, practitioner and policy communities seem either disinterested or under the mistaken perception everything related to intelligence is secret and therefore unimpeachable outside classified forums.

To date, neither the intelligence community nor the homeland security community has adequately articulated, defined, or implemented a comprehensive or agreed upon role for intelligence in homeland security decision-making processes (DHS, 2007, p. 9). While the anticipated benefits of services for operational enablers, such as communication, medical, logistics, etc., are generally within common experience of most homeland security leaders and practitioners, the role of intelligence in homeland security seems to be less well understood or appreciated, especially among non-law enforcement professionals (Interagency Threat Assessment and coordination Group [ITACG], 2008). As the role (and subsequent value) of a lawyer or a dentist becomes acutely relevant for leaders and practitioners facing legal challenges or dentine sensitivities, the role and value of intelligence seems largely underappreciated or misunderstood until a major threat manifests or a crisis erupts. I submit the potential revolutionary benefits for

homeland security leaders and practitioners using intelligence cannot be gained when called upon intermittently or only when "trouble" arises, especially in an age of constantly evolving asymmetric threats of previously unimaginable consequences. The efficacy of intelligence in promoting decision advantage as an "on demand" capability is severely reduced in an environment of persistent and lethal threats. The acquisition and maintenance of an adaptive threat orientation is as much or more the responsibility of the consumers of intelligence as it is intelligence producers. Occasional or intermittent usage of threat knowledge of an asymmetric, adaptive, and cunning adversary within the dynamic and complex threatscape of homeland security is wholly inadequate to facilitate persistent and agile decision advantage and is likewise an unnecessary and entirely preventable invitation for disaster. Failure to appreciate and incorporate the role of intelligence in homeland security decisions may impede efforts to eliminate loss of opportunity, wasted resources, violations of civil or human rights, or potentially undue loss of lives and property.

Homeland security objectives are not advanced when "intelligence knows" something as "intelligence" does not make decisions necessary to advance those objectives. In order to be most effective and efficient homeland security decision makers must understand how threats within their areas of responsibility (geographic, jurisdictional or otherwise) effect their operations and objectives. This understanding can come from two sources 1) direct contact with the threat or 2) intelligence. When intelligence is framed as such, the mystic veneer attributed to intelligence fades and the intelligence professionals and homeland security leaders and practitioners are in a better position to focus on creating processes and relationships that facilitate the need for timely, accurate, and tailored threat understanding.

B. RESEARCH QUESTION

What are the roles and benefits of intelligence in acquiring and maintaining homeland security decision advantage?

This thesis seeks to identify and examine specific and compelling roles for intelligence in acquiring and maintaining homeland security decision advantage as well

as the anticipated benefits derived the from acquisition and maintenance of an intelligence-based decision advantage. Research was ordered around the following questions:

- *What* are the roles of intelligence in acquiring and maintaining homeland security decision advantage?
- *What* are the derived benefits of intelligence-based decision advantage for homeland security leaders and practitioners?

C. METHODOLOGY

Grounded theory is the research methodology chosen for this thesis. Grounded theory proposes the traditional concept of asserting and defending predetermined theses has the potential to negatively bias the use of research data by wittingly or unwittingly "channeling" data and observations towards an intended hypothesis or persuade a researcher to disregard an emergent theory that fails to prove or disprove his or her thesis (Borgatti, 2009). Grounded theory is well suited for the broad nature of these research questions, as the research objectives had the potential to, and ultimately did, spring from the wide depth and breadth of research required for this method. The research approach for this project began with a thorough examination of multi-source video, audio, and print materials across the intelligence, homeland security, decision science, technology, legal, historical, information management, cultural, naturally occurring networks; including military, business, and academic fields of study to identify and distill the "raw materials" useful for homeland security leaders and practitioners wanting to improve decision quality.

During the topical analysis of the data, elements and theories were captured and tracked using selective coding, loosely based on the research questions. This liberal research process provided an appropriate mix of creative research opportunity and specific content capture without stifling potential elements as they emerged. The coding structure loosely followed the two primary research questions.

After research notes were coded and analyzed for applicability to the research questions, the elements were sorted and combined as potential solution sets for the research questions. Subsequently, each solution set was analyzed and evaluated for

relevance to the research questions and then drafted as subcomponents of the emergent theses. Lastly, the component parts of the coded and analyzed research were grouped, ordered, and ultimately prioritized according to the analytical arguments and evidence discovered.

Analysis of this data within the context of the research questions resulted in the hypothesis that while certain expected functions of intelligence were universal (mitigating surprise, reducing uncertainty, etc.) homeland security leaders have differing expected applications (use) for intelligence depending on their own roles within the homeland security enterprise (political, operational or tactical). The use of grounded theory supported the evolution of the hypotheses that use of intelligence can have political, legal, psychological, and even barter value in addition to more commonly appreciated.

D. LITERATURE REVIEW

The broad and eclectic nature of this research provided both a unique opportunity and a considerable challenge in relation to analyzing such an expansive topic aperture of literary and media sampling. The research literature was classed for analysis into two primary categories: 1) reasons why intelligence may be useful in acquiring and maintaining homeland security decision advantage and, 2) the identification and examination of potential derived benefits of intelligence-based homeland security advantage.

The topical areas reviewed were: 1) the use of intelligence as a practice and as a process, 2) homeland security generally, 3) homeland security intelligence, 4) decision science and psychology, 5) law and policy, and 6) political applications.

1. Literature on the Use of Intelligence

The volume of literature with respect to the production of intelligence for national security decision making is generous (Treverton & Gabbard, 2008; Reveron 2007). This literature commonly falls into roughly one of two categories, 1) the field of intelligence as a practice (production and analysis) or, 2) historical and reform driven literature. The

largest sample of literature suggesting specific reasons decision makers would want or need to adopt intelligence as a factor in their decision-making, relied chiefly upon biographical anecdotes, not quantitative research (McNeil, 2008). Much has been written on how to "fix" intelligence, yet little scholarship exists on how to implement this "fixed" intelligence into homeland security decision-making processes, especially in organizations that have not previously been involved in using intelligence as a factor in decision making (Treverton, 2001).

The most prolific arguments for the use of intelligence in decision making appeared targeted toward military and national security decision-making policy and doctrine (Department of Defense [DoD], 2008; Department of the Army, 1994; Wolgast, 2005). Other than exhortations to use and engage the intelligence community, this literature review was notably devoid of suggestions for practical reasons or coherent correlations for homeland security decision makerss on how they might use intelligence (Steele-Vivas, 1996; Langerman, 2007).

2. Literature on Homeland Security Policy and Intelligence Generally

The *National Strategy for Homeland Security* and the *Department of Homeland Security Intelligence Strategy* provide the most comprehensive government literature on federal government policies with regard to situations homeland security leaders may seek to incorporate intelligence (White House, 2007; DHS, 2006). However, neither of these documents specifically articulate the benefits (or value) of incorporating intelligence into decision-making scenarios.

3. Literature on Intelligence in Support of Homeland Security Objectives Generally

In order to successfully prevent and disrupt terrorist attacks, homeland security decision makers at all levels require timely, accurate, and useful threat knowledge specifically tailored to their decision spaces. Published government plans and policies and scholarly literature on homeland security prevention tactics, techniques, procedures and policy are underwhelming in their lack of attention to the role intelligence can play at the state, local, and tribal levels. The *National Strategy* (White House, 2008) spends a

mere eight of 53 pages discussing prevention and disruption policy, but mentions intelligence only six times, all of those references within the section on disrupting terrorists within the United States. The lack of progressive application of intelligence with community-wide prevention efforts may be indicative of both high-level policy ambivalence as to the value of intelligence in preventing terrorism and a widespread misunderstanding of how intelligence can proactively shape prevention decisions at tactical and operational level.

4. Literature on Intelligence in Support of Homeland Security Prevention Efforts

According to national level plans and doctrine, in order to offer adequate protection, first policy makers must initially decide both what to protect, and from which threat to focus the protection against (DHS, 2007). Again, intelligence is woefully underrepresented in the policy literature on both aspects in the *National Strategy for Homeland Security* (White House, 2008). While a host of homeland security threats are widely discussed by name (including infectious diseases and catastrophic public health threats, and attacks against critical infrastructure and key resources) no mention was found of the value of incorporating intelligence on those threats into protection planning or efforts (DHS, 2007).

5. Literature on Intelligence and Homeland Security Response

A significant body of literature has been generated regarding the policies and strategic solutions developed by the government in partnership with state and local agencies to respond uniformly (such as the *National Incident Management System* (Federal Emergency Management Agency [FEMA], 2003) and the *National Response Framework* (FEMA, 2008)); however, the value of incorporating intelligence into response options and activities is referred to peripherally as obtaining situational awareness (FEMA, 2009). Several authors have explored and advocated for the potential for military intelligence support (intelligence, surveillance, reconnaissance assets and personnel) for "battle damage assessment" type assistance in order to provide situational awareness to commanders (Anderson, 2005). This literature, however, centers

predominantly within The Department of Defense (DoD, 2006) and United States Northern Command (USNORTHCOM) and Department of Homeland Security intelligence collection and analysis efforts with a focus on meeting the strategic intelligence requirements of national level decision makers first, and operational and tactical level decision makers on an "ad hoc" basis.

6. Literature on Homeland Security Intelligence

Literature on homeland security intelligence, as a practice, seems to mirror that of the other intelligence writing with regard to the application of intelligence to the decision-making process. This ought not to be surprising since a significant segment of the intelligence literature drafted after 9/11 was written by authors and academics laboring in the same or similar fields prior to 9/11. I found Gregory Treverton's (2009) book *Intelligence in an Age of Terror* the most noteworthy post-9/11 manuscript regarding the use of intelligence within the current political and operational environments.

As for literature suggesting explicit rationale why homeland security leaders specifically should value intelligence, none was identified.

7. Literature on the Decision Sciences

The decision sciences provide seemingly endless models on how to improve decision quality; however, no literature was noted suggesting any specific research or commentary on how homeland security decision makers across the spectrum are integrating intelligence into their decision-making processes (Masse, 2006). On its face, decision science provides little insight into how intelligence specifically can be used to improve homeland security decisions. Decision science did provide scientific evidence that was used by extrapolation as reasoning for the use of intelligence to improve decision-making generally (Krawchuk, 2000; Davis, Kulick & Enger, 2009). Various threat and opportunity models were also examined, that when carried by extension to the homeland security decision space, may provide sound reasons for incorporating intelligence (Shambach, 1996; Mitchell & Decker, 2004). The field of decision science is amply populated with literature on incorporating various factors into the decision-making

process, but the field is noticeably silent on the incorporation of threat knowledge per se (Zsambok, Klein & Beach, 1992). The fundamentals from which the author's adaptive threat orientation model are derived spring from military strategist John Boyd's (1995) "Observe-Orient-Decide-Act Loop" or "OODA" Loop.

E. REASONS FOR INTELLIGENCE USE

1. Legal Reasons for Intelligence Use

Although secondary in impact to the operational security objectives of homeland security leaders, the legal and political uses of intelligence should be regarded as both valid and invaluable reasons to use intelligence.

As a nation of laws, leaders, practitioners, and citizens are expected to operate within the bounds of the law. A review of intelligence law uncovered a wealth of opportunities and restrictions for the access and incorporation of intelligence into decision-making processes. The *Intelligence Community Legal Desk Reference* (Office of the Director of National Intelligence [ODNI], 2007) and the legal treatise *National Security Law* (Dycus, Berny, Banks, & Raven-Hanse, 2002) provided rich statutory, common law, and commentary for the legal applications of intelligence.

A healthy and passionate debate can be found with regard to the issue of domestic intelligence gathering, analysis, and dissemination, with equally enlivened arguments on either side. Intelligence law literature was classed into statutory, executive branch (administrative rulemaking), common law (rulings of the court), or commentary on any or all of the aforementioned writings.

2. Political Reasons for Intelligence Use

Most of the literature reviewed on the political use of intelligence was generally of a conspiratorial, or "exposé" nature, suggesting that the use of intelligence for political purposes is disfavored by scholars and citizens alike (Warrick, 2008; Lawson, 2008). Withholding moral judgment on the political uses of intelligence, it is important to note that while much of the popular literature and media disfavored the use of intelligence for purposes other than security, many political scientists and communication theorists

propose a rather "to the victor--the spoils" attitude of parties in power using all methods within their power to retain such power, intelligence being no more immune than any other information that might further the interests of the moving political party (Cutler, 1993). Angelo Codevilla's *Informing Statecraft* (2002) was an excellent resource in describing potential opportunities within the U.S. State department and U.S. Senate on how intelligence might be of use to policy makers within their respective roles.

F. FUTURE RESEARCH

This thesis may be useful in shaping future discussion and research on the topics of the practice, use of information sharing systems and products, intelligence gathering, intelligence analysis, and incorporating intelligence into homeland security decisions. This thesis may also drive much needed focused research on the impact of homeland security intelligence requirements on the intelligence community as well as, the security, technological, or policy implications of expanded incorporation of intelligence into other non-homeland security decision processes.

By examining and parsing out critical elements of what a successful intelligence incorporation model might include, homeland security leaders may in turn leverage these "proto-doctrine" building blocks to create their own intelligence incorporation doctrine according to their own specific homeland security responsibilities and constraints instead of pursuing a "one size fits all" federally mandated or nationally propagated homeland security intelligence (HSINT) doctrine.

Scrutinizing the value of intelligence from the production perspective may also provide impetus for the Intelligence Community to adjust their collective cultural paradigm away from a mindset of "production" of homeland security intelligence as if it were a just another product, to a new standard of intelligence as a process of orientation to a threat or opportunity. Additional research into emerging intelligence application foci, departing from a product foucs, and leaning towards the actual use, implementation, and impact of knowledge and understanding of a threat or opportunity within the decision space of a particular homeland security leader may also greatly benefit both communities.

G. INTENDED CONSUMER

The intended audiences for this research are homeland security leaders and practitioners interested in improving their decision quality; who may, or may not, have experience as a consumer or participant in the intelligence process. Other individuals that may benefit from these ideas are homeland security and intelligence community leaders, and policy makers tasked to provide value-added intelligence products, systems, and programs to the homeland security community.

The remainder of this thesis is organized in three chapters: 1) the role of intelligence in homeland security, 2) how homeland security decision advantage is acquired and maintained, and 3) an examination of the specific derived benefits of intelligence-based decision advantage for homeland security.

II. THE ROLE OF INTELLIGENCE IN HOMELAND SECURITY

> The key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision maker's quandary and allow him to act. **This ability to lubricate choice is the real objective of intelligence** [emphasis added].
>
> Jennifer Sims (ODNI, 2008, p. 8)

A. OVERVIEW

Intelligence cannot eliminate uncertainty in the unordered decision space that is homeland security. This is an unattainable and unrealistic objective, as the unknown factors driving change within the space include the thoughts and intentions of small groups of highly networked individuals, or even solitary actors. Intelligence is valuable when it contributes to a threat understanding "end state" wherein "uncertainties about the adversary and anxieties about vulnerabilities should lessen" (Turner, 2005, p. 6). Turner (2005, p. 13) continues, adding that intelligence increases its value by "tempering" uncertainty when the collective intelligence efforts have "reduce(d) uncertainty…to the extent that viable options and opportunities are identifiable and made available for policy leaders."

The value of intelligence to homeland security decision makers may be succinctly categorized into three benefit classes: 1) define the proximate threat reality, 2) mitigate the negative effects of surprise by facilitating foreknowledge of the threat, and 3) optimize homeland security opportunities, policy and resources within the threat environment. Decisions in the uncertain homeland security threat environment require judgment, and judgment with the benefit of tailored, timely and accurate intelligence can greatly increase the potential for desired outcomes within an uncertain decision space.

B. CRITICAL TERMS AND DEFINITIONS

Certain terms and definitions will be used throughout this thesis, many of which have different meanings in practice across the many disciplines of homeland security and intelligence. In the interest of consistency the following terms will be used throughout this thesis according to the definitions provided.

- **Threat:** A potential for an individual or group to exercise an action that exploits vulnerability. It does not automatically imply the level of danger that exists (Dictionary.com, 2010).
- **Vulnerability:** A flaw or weakness that can be exploited by an attacker (Dictionary.com, 2010)
- **Risk:** The probability of harmful consequences arising from an action taken by a source to exploit a known vulnerability (Quiggin, 2007, p. 25).
- **Decision Advantage:** the circumstance or factors that place one in a favorable position in relation to the judgment associated with coming to a conclusion or determination (Aftergood, 2008).
- **Intelligence:** Intelligence is the process and products that account for how an organization knows about threats prior to direct contact with the threat (Author, 2010).
- The *United States Code* (50 U.S.C. §401a(5)) is helpful in illuminating the legal definition of *national* (but not homeland security) intelligence as:

  > information gathered within or outside the United States, that pertains…to more than one…agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

- **Value of intelligence:** Value can be defined as the worth, or importance, or usefulness of something to somebody (Encarta.com, 2010). When intelligence is valued decision makers find the costs associated with threat observation and orientation worth the benefits derived from the resultant threat understanding and potential decision advantage.

  How threat knowledge is used (or disregarded) by decision makers is not intelligence, but rather a function of decision-making processes (Wheaton, 2010).

- **Role of intelligence:** A role can be defined as a specific function, the usual or expected function of something, or part something plays in an action or event (Encarta.com, 2010). As such, the role of intelligence in acquiring and maintaining decision advantage is only one of many usual

> or expected functions necessary for advantage to occur. The purpose or function to which homeland security leaders employ or accept intelligence as part of their decision-making processes will depend directly upon the decision makers experience and understanding of intelligence, homeland security, and threats.

C. HOMELAND SECURITY INTELLIGENCE—TO WHAT END?

Seekers of Wisdom first need sound intelligence

Heraclitus

The Department of Homeland Security asserts that intelligence is central to "everything homeland security does" (Allen, 2006, p. 2); yet the intelligence branch of the Department of Homeland security receives a pittance of the national intelligence budget and is held with minimal regard within the intelligence community (Gorman, 2005). Factors such as this suggest an inconsistency between what the homeland security community writ large *says* about intelligence, and the actual role of intelligence in how homeland decisions are being made and the amount of value the homeland security community *expects* or *derives* from intelligence it receives. Contrary to the rhetoric, revolutionary improvements to homeland security decisions cannot come from improved intelligence alone; this progress can only come from improved homeland security decisions. "Fixing" homeland security intelligence, will not "fix" homeland security. While it is true that "better" intelligence may result in a more informed intelligence community, without "better" use of intelligence by homeland security decision makers the opportunity for improved homeland security decisions may be wasted. The answer to "homeland security intelligence, so what?" must unequivocally be "decision advantage."

Homeland security is not "national security-lite," and the static and symmetric security policies, doctrines, and practices that served the nation widely and well during the Cold War are wholly inadequate in their unaltered or mismatched application within the contemporary homeland security domain. A very real concern is threats previously considered ***uncommon*** within the U.S. (such as weapons of mass destruction or terrorist attacks against civilians) are largely being addressed by ***common*** responses, without acknowledging either the complexity or consequences of these new threats or the potential opportunities for optimization of resources and policy. The "new" homeland

security reality is one of asymmetric threats with potential catastrophic consequences that previously had been considered exclusively foreign threats (to be dealt with "over there"). Advantageous homeland security policies require new thinking about these new challenges, within a relatively new threat environment—American soil. Homeland security intelligence (HSINT) is both the manner and mechanism by which the American people, public and private industry, and government homeland security leaders and practitioners can acquire and maintain domestic threat understanding. After considering *why* intelligence is critical to informed security judgments, homeland security decision makers may more artfully and effectively entertain options for, *when*, *where*, and *how* they will plan, program, train for and execute the inclusion of intelligence in their own decision processes.

D. HOMELAND SECURITY INTELLIGENCE (HSINT) SUMMARIZED

- Homeland security intelligence is threat data and information that has been analyzed and deemed significant to the goals and purposes of homeland security decision makers. It is knowledge about adversary capabilities and intentions beyond a homeland security decision maker's control or common experience. HSINT is both the process and products within the scope of knowledge related to homeland security threats.
- Homeland security intelligence is derived from multiple collection means and sources and typically specializes in using "dirty" data (incomplete, unstructured, and deceptive) as a basis for analysis and assessments. HSINT is more than just "secret" intelligence; it relies on observation and orientation (analysis) from across the homeland security and national security enterprises, as well as private sector, media information.
- Homeland security intelligence primary operational role is to reduce the level of uncertainty within the homeland security decision space. More than "pure research" or "pure journalistic reporting," HSINT must support the homeland decision-making process and do so in persistent and credible ways.

III. ACQUIRING AND MAINTAINING INTELLIGENCE-BASED HOMELAND SECURITY DECISION ADVANTAGE

> *Decision advantage results in the ability of the United States to bring instruments of national power to bear in ways that resolve challenges, defuse crises, or deflect emerging threats.*
>
> Jennifer Sims (ODNI, 2008, p. 8)

A. GENERATING DECISION ADVANTAGE: FROM OBSERVATION TO ADVANTAGE

The value of decision advantage in violent contests has been established since the very earliest records of the physical struggles of man (Sun Tzu, 2002). Mansdorf and Kedar (2008) assert in the contemporary homeland security threat environment the asymmetric nature of the terrorist threat presents an extreme example of the importance of understanding well ones' adversary, as knowledge, not forces or logistics is the life blood of asymmetric struggle. In order to effectively combat asymmetric adversaries, homeland security leaders and practitioners must organize and plan homeland security strategies and policies, as well as recruit, train and equip personnel able to optimize knowledge of the adversary while denying the enemy as much information as possible that may be advantageous to their adversary's desired effects.

Homeland security decision advantage results in the ability of homeland security enterprise leaders and practitioners to bring instruments of national, state, local, tribal, private enterprise, and individual citizen powers to bear in ways that resolve homeland security challenges, defuse homeland security crises, or detect and neutralize emerging homeland security threats. Although a term of relatively new usage for intelligence professionals and security decision makers, decision advantage is now considered the "enduring mission" of the United States Intelligence Community (Turner, 2005, p. 1).

B. THE VALUE OF INTELLIGENCE FOR DECISION ADVANTAGE

The root challenge facing our security apparatus is uncertainty.

Richard A. Posner (2005, p. 2)

Homeland security leaders and practitioners (collectively) lack neither the cognitive capacity nor active interest in threats to perform their own analysis, nevertheless in a crisis situation, they are not likely to have the time, accesses or luxury of singly focusing attention on those threats. The sheer volume of threat data and intelligence produced in response to a homeland security event could easily overwhelm anyone unaccustomed to distinguishing consumer specific threat signals from the "noise" of the strategic, operational or tactical environment.

In the complex homeland security environment, it is a leader's and practitioner's attention, not intellect or information may be the asset of greatest demand when attempting to navigate within a constantly changing threatscape. The most inopportune time to become aware of or oriented to an imminent threat may very well be at the same time one is trying to coordinate ongoing prevention, protection, or response operations. The demands on time and attention necessary to observe and orient to threat developments within the threatscape, present possibly the single greatest justification for why homeland security leaders and practitioners need to rely on intelligence professionals to assist them in acquiring and maintaining an adaptive threat orientation.

Intelligence plays a critical role in determining how homeland security decision makers become aware of threats within their operating environment. The following analysis examines principles by which homeland security leaders and practitioners may rely upon to convert intelligence into decision advantage.

C. FOUNDATIONS OF DECISION ADVANTAGE: FROM DATA TO VALUE

Intelligence produces masses of data, the import of which is clear only to people educated to understand it.

Angelo Codevilla (2002, p. 15)

1. Intelligence Creation Process

The production of intelligence is a three part process: 1) data is collected through observation, 2) that data is converted into information by analysis and the 3) analysis becomes potential understanding to an intelligence consumer through creation of a deliverable (report or briefing) that can be applied to a specific decision or problem set within the threat environment (Quiggin, 2007, p. 52) (see Figure 1).

Table 1. Intelligence Creation Process (After Codevilla, 2002, p. 52)

Data: most basic form of observation/collection; has not undergone any form or processing or analysis
Information: Primary level of processing, organized in such a way as a human being can derive benefit from exposure.
Knowledge: the application or judgment of information in the context of previously understood information.
Understanding: an appreciation for causal and consequential relationships between information through application.

Threat factors "known" (i.e., observed and analyzed) by the intelligence producers but "unknown" (i.e., not disseminated or understood within the context of the organizational objectives) to decision makers not only frustrates the purpose for intelligence in the first place, it can result in unnecessary and potentially catastrophic errors of judgment, either due to lack of threat understanding or in unnecessary operational delays waiting for intelligence that is unknown or unknowable (Rumsfeld, 2002).

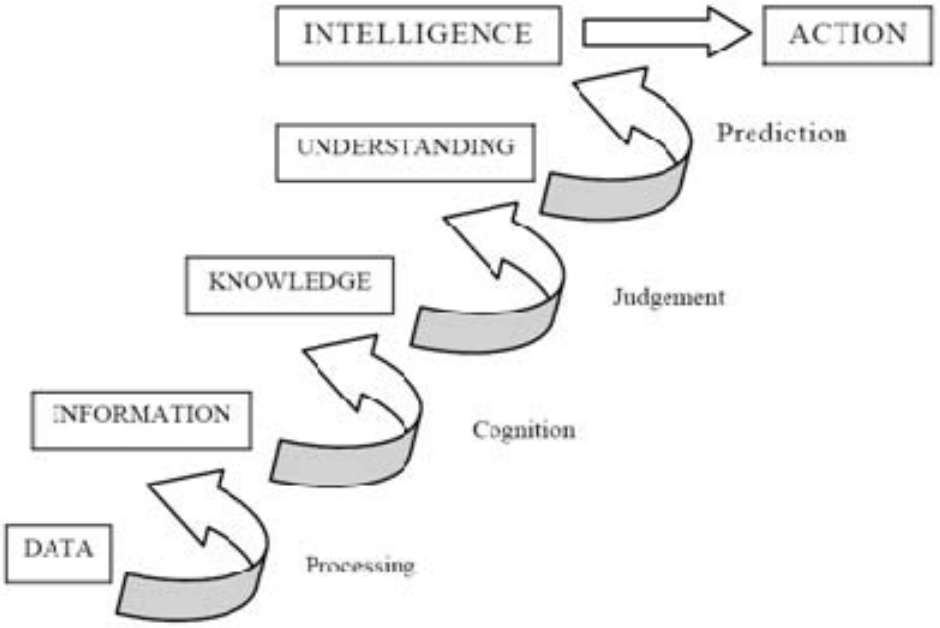

Figure 1. Intelligence Data to Action Model (From Cox, 2004, p. 11)

After knowledge has been created and to be valuable to decision makers, it must be brokered, bundled, exported, imported and then presented to a decision maker for consideration (Deptula, 2008). Arguably, the most significant failures and inconsistencies in the security community are in the brokering, bundling, exporting, importing and presenting of knowledge to decision makers, **not** in the creation of **more knowledge**. Inversely, the greatest opportunities for revolutionary advances in improved homeland security decision making may be derived from improved brokering, bundling, exporting, importing and presenting of knowledge to decision makers, not in the creation of more knowledge (see Figure 2). An unwarranted amount of focus within the intelligence community appears to be on observation and production of reports, and not on the actual orientation of decision makerss to that threat knowledge (Sims, 2007, p. 8).

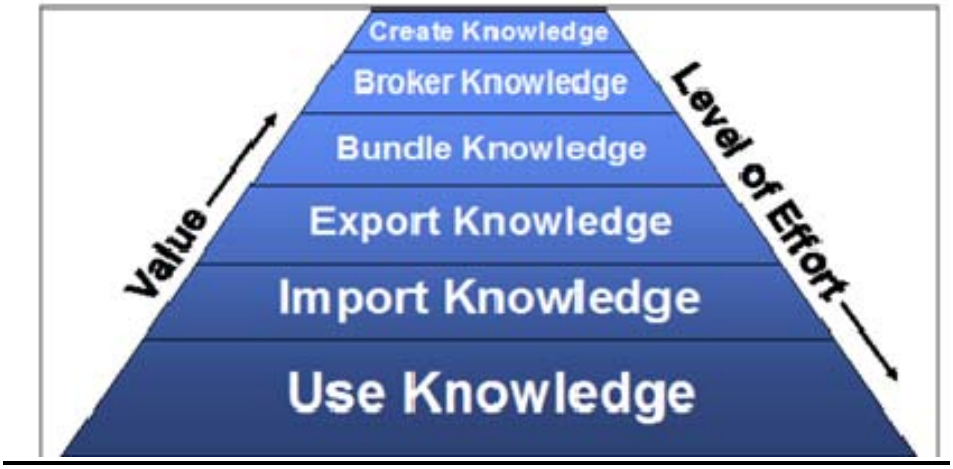

Figure 2. Intelligence Value to Effort Ratio Model (From Deptula, 2008)

If intelligence is "central to everything" that homeland security leaders and practitioners do, then these decision makers must create and resource adequate programs and processes designed to not create threat more knowledge but to **optimize** the **impact** of threat understanding across the homeland security decision space.

D. MAINTAINING DECISION ADVANTAGE REQUIRES AN ADAPTIVE THREAT ORIENTATION

The homeland security decision-making environment is a complex and dynamic environment as data in relation to potential threats is deliberately deceptive or difficult to observe, and the threat, left unchecked has the potential for great destruction or disturbance, often without warning. Homeland security decision makers with an appreciation for the value of intelligence will rely on trained threat observation and orientation professionals to continually survey the threat environment with the specific objective of ultimately not producing reports, but orienting specific decision makers to specific threat dispositions as the tactical, operational, or strategic circumstances dictate. Homeland security decision makers may then integrate this understanding into their efforts to determine potential challenges or opportunities, gauge the expected efficacy of current or pending security efforts, evaluate probability of desired outcomes within the threat environment, consider potential courses of action in light of the changes within the

threat environment, decide on courses of action, and then guide into action in light of the threat's capabilities, limitations and intent.

1. Towards An Adaptive Threat Orientation

> *Decision makerss do not need the broadest range of possibilities; they need a relevant range of the most likely probabilities. The intelligence process produces such a range.*
>
> Brigadier General James Cox (2004, p. 19)

If the purpose of intelligence is to orient decision makers to the threats within a given environment, programs and processes must be developed and implemented that create a sustainable level of orientation in light of changes within that environment. Homeland security decision makers that pursue and adopt an adaptive threat orientation to maintain their decision advantage are more likely to acquire and preserve a timely and accurate threat understanding, than those who do not. With this flexible and adaptive understanding these leaders and practitioners will be more aware of and thus have a more proximate understanding of the risks to his or her organizational objectives prior to engaging in his or her decision-making processes. As such, these decision makers stand a much better chance of more capably arriving at risk based decisions and maximizing the homeland security resources and opportunities than those who do not seek or provide for this adaptive threat understanding standard.

Without the use of intelligence, chance may take the place of knowledge, and waste the place of economy. Therefore, an operational "end" for homeland security intelligence is in the creation and maintenance of sustainable decision advantage against threats to homeland security objectives through an adaptive threat orientation.

2. The Value of *Adaptive* Threat Orientation in Sustaining Decision Advantage

> *The judgment of a trained and experienced mind will be more likely to get things right then the judgment of a mind lacking those qualities.*
>
> Walter Laqueur (1999, p. 308)

An adaptive threat orientation is a threat ontology framed to quickly "create domain-level context that enables users to attach rich domain specific information and additional annotations to intelligence information" (Raghu, Ramesh, & Winston, 2005, p. 312). Because this orientation "posture" is adaptive, it is never complete but requires continuous observation of the operational environment, actively seeking threat signature information from all available indicators that may drive adjustments within the organizations' operations or resource allocation according to the changed conditions. Decisions are made in light of the threat and driven by security goals that exist because of known or anticipated threats within a specified homeland security environment. Since an adaptive threat orientation is as much the capacity to acquire and apply threat knowledge within an organizational decision space for the purpose of attaining decision advantage as it is a desired end state, an adaptive threat orientation can become both a goal and a framework from which decision makers can organize their intelligence operations (observation and orientation).

3. Why Adaptive?

The threat environment of homeland security is laden with uncertainty and rapidly changing unordered challenges. As such, many homeland security threats do not submit to data for analysis as more symmetric or ordered challenges might. Unordered challenges do not have "yes or no" answers that can be deduced from the facts, due to the swift rate of change and the deliberate obscurity of the factors upon which decisions might be based. In order to best posture potential security courses of action for success, homeland security decision makers must realize that "the right answer" to security questions only remains "right" as long as the threat factors from which that decision is was based upon remain unchanged. Change in the homeland security environment can occur as fast as potential threat actors are able to think and communicate.

The asymmetry and intrinsic adaptability of homeland security threat tactics, techniques and procedures, in addition to seemingly limitless targeting possibilities, demands sound homeland security policies, tactics and procedures be equally as adaptive as the threats they face. Both decision makers and intelligence professionals must

understand and operationalize practices conducive to the principle that intelligence is only "good" for as long as the observations and analysis by which it was created remain unchanged. A central role of intelligence is to track (i.e. observe) and inform (i.e. orient) when these changes occur, especially those changes with immediate or significant consequences within a homeland security decision maker's decision space. Without intelligence there is no foreknowledge of the threat. Without foreknowledge of the threat there can be no threat orientation. In the absence of this orientation, security decisions may be made without regard to the very threats they contend to address.

Complex dynamic systems theories, like the adaptive threat orientation, provide an example of a pragmatic foundation for thinking about the homeland security threat environment (Abraham, 1998). The hyper-consequential homeland security environment mixes both complexity (and as a result uncertainty) and dynamism in a way uncommon in contemporary U.S. domestic security. Complex dynamic systems are better suited to account for the one extremely important aspect of the environment that linear and cause-effect models fail to realize: environmental rate of change (Underwood, 2002). When dealing with the uncertainty of terrorism or other homeland security threats, not having an adaptive mindset can hamstring, if not cripple, decision makers when threat changes inevitably manifest within the homeland security environment.

4. Decision Advantage and Psychological Enabling

> *Intelligence remains information, no matter how adroitly collected, and no matter how well analyzed, until it is lodged between the ears of a decision maker.*
>
> General Paul Gorman (USA Ret) (Senate Hearing, 1992, p. 262)

One of the foremost values of intelligence to the homeland security community is to prepare the minds of decision makers operating within this specific and unique threat environment of the inherent threat variables and potential consequences of security actions (from the adversary's perspective) taken within those threat circumstances. Even with an adaptive understanding of the threat (and how that threat applies to the decision space), significant psychological barriers may exist, which if not overcome, can also lead to suboptimal decision outcomes. By understanding threats within a perspective of

awareness and orientation, decision makers can avoid falling into the "connect the dots" fallacy so commonly referred to as a function of intelligence (Mata, 2010). Because homeland security organizations seek to achieve their objectives within a rapidly changing operational environment, often pitted against highly adaptive adversaries with competing or destructive intent, there is no static "picture" per se that intelligence professionals can form by "connecting the dots." The "threat picture" can change as rapidly and often as the tactical, operational and strategic environments change, potentially at the speed of thought when it comes to intentions or targeting. The importance of intelligence in overcoming negative psychological effects will be examined further as an independent benefit of intelligence-based decision advantage.

5. Decision Advantage and the "Observation and Orientation Decide Act Loop"

In his revolutionary presentation *Organic Design for Command and Control* (1995), military strategist John Boyd proposed the key to decisive combat success was not in strength or power ratios but in the maneuverability, speed and nimbleness in which decision makers could observe and orient themselves to the environment and make decisions and take action according to that environment. This decision-making paradigm flew in the face of hundreds of years of western military doctrine (e.g., Clausewitz) and legitimized within the United States military establishment the more eastern focused theories that centered on "out thinking" rather than "out gunning" ones' adversaries.

The Observe-Orient-Decide-Act (OODA) loop (Figure 3) is the diagram that encompasses Boyd's decision theory. In the "hurry up and do something" environment that too often grips the homeland security community, the OODA loop offers unique insight into the importance of the intelligence functions of observation and orientation.

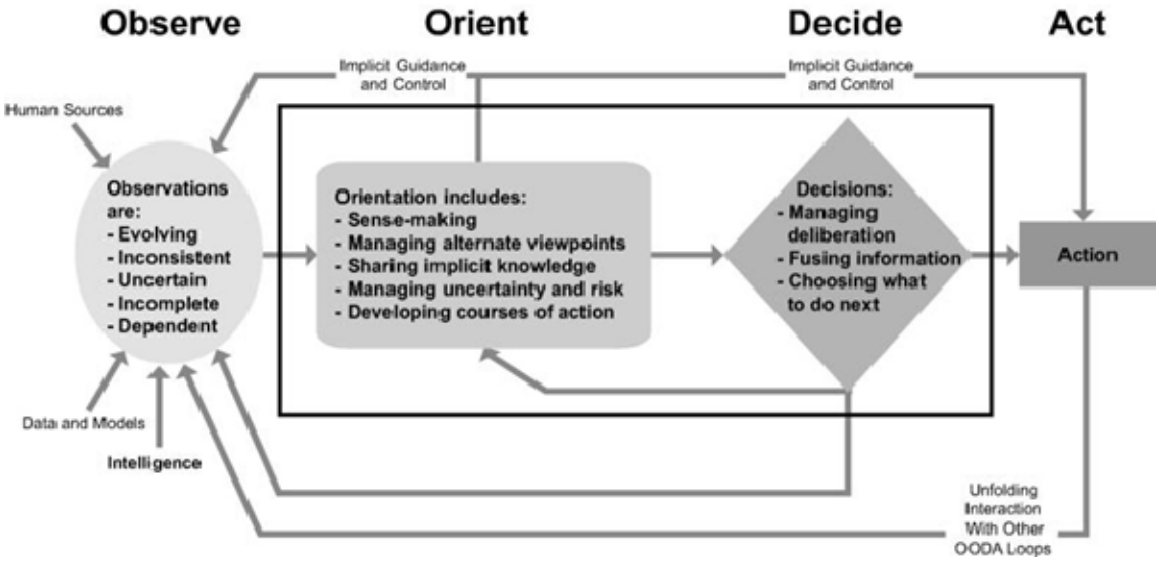

Figure 3. Observe-Orient-Decide-Act Loop (From Boyd, 1995)

According to Boyd:

> The second O, orientation—as the repository of our genetic heritage, cultural tradition, and previous experiences—is the most important part of the OODA loop since it shapes the way we observe, the way we decide, the way we act. (1995, slide 4)

In the context of homeland security decision making, the value of intelligence as orientation is in swiftly and wholly incorporating changes within the threat environment, moving intelligence "inside" the loop and actually adopting it as part of the way homeland security decision makers think about the decisions they make and the consequences of actions taken.

6. Decision Advantage and the Orientation Gap within the Intelligence Cycle

The final stage of the "official" intelligence cycle is the dissemination phase (Krizan, 1997, p. 7). As soon as reports are delivered and "intelligence needs" (requirements) are met, the process resets to meet other intelligence needs and assumes upon delivery, that the intelligence obligation is met. This "result" puts more of a focus on production and dissemination of information than orientation about what the

intelligence might actually mean for that decision maker in the context of their specific threatscape and objectives. Reasons for this arm's length association abound; but most stem from a fear that too close of a affiliation between decision makers and threat information providers will somehow skew the intelligence to suit decision maker's desired outcomes(Kent, 2003). This "delivery" process has significant limitations for homeland security decision makers because of the steep learning curve and breakneck speed of change associated with homeland security threats. Intelligence, whether as product or process, is not self-evident or self-executing. For homeland security leaders unfamiliar with the intelligence process or unpracticed in relying on rapidly changing or imperfect threat information in a decision process, the mere delivery and possession of intelligence does not help to create threat understanding and is therefore of limited or even negative value if decision makers have an unrealistic expectation of intelligence or they are "holding out" for "smoking gun" type intelligence that may never manifest.

In much the same way it would be inappropriate for homeland security lawyers to respond to legal questions pertaining to the homeland security decision space by dropping case law or statutes on a decision makers' desk and then retreat back to their offices to research and draft more memos, it is likewise absurd to assume that the intelligence function of orientation can be accomplished by dumping intelligence reports on a decision makers' desk or inbox and then retreating back to produce more reports. Constant and robust dialog between decision makers and intelligence professionals regarding both changes within the security operations environment, and changes within the threat environment is incontrovertibly critical to the successful optimization of intelligence within homeland security efforts to achieve decision advantage. The analytical bridge spanning the gap between knowledge creation and homeland security decision advantage is the acquisition and maintenance of an adaptive threat orientation.

7. Decision Advantage: Summary

The value of decision advantage should be of paramount importance to homeland security leaders and practitioners. In the highly complex and consequential environment that is homeland security, no advantage can be ceded to the adversary. Like intelligence,

decision advantage for its own sake is without impact. Decision must lead to action, and action must yield desired effect to be considered successful.

The following section identifies and examines six derived benefits of intelligence-based decision advantage for homeland security leaders and practitioners.

IV. SIX DERIVED BENEFITS OF INTELLIGENCE BASED DECISION ADVANTAGE FOR HOMELAND SECURITY

> *We have to accept the fact of uncertainty and learn to live with it. No magic, no code, or otherwise will provide certainty. Our plans must work without it.*
>
> Roberta Wohlstetter (1962, p. 400)

This section identifies and elaborates on six specific categories of benefit is homeland security leaders and practitioners might expect from intelligence-based decision advantage. I submit the homeland security enterprise should fund, organize, equip, train, and rely on intelligence for six primary purposes:

1. To mitigate the negative effects of surprise,
2. Depict proximate reality,
3. Optimize resources,
4. Make risk-based policy and legal decisions,
5. Overcome detrimental psychological and decision biases and,
6. Provide commodity and symbolic value to homeland security intelligence consumers.

Additionally, these "fruits" of intelligence can provide consumers with a context from which they can measure the effectiveness and value of the intelligence support they receive. Consumers may evaluate intelligence within this framework as well as provide specific feedback to homeland security intelligence producers as to the detailed efficacy of certain products or reports.

If not for the uncertainty inherent to the homeland security environment, the costs in resources and potential limitation of liberties proposed by the security community may be difficult to justify. The first part of this section seeks to define and examine the specific values of intelligence as a "tempering" agent in a chaotic and untempered decision space.

A. MITIGATE SURPRISE

A commander may be excused for being defeated but never for being surprised.

U.S. Army Cavalry Manual (Department of the Army, 1935 p. 5)

The primary benefits of homeland security intelligence in mitigating surprise are two-fold: 1) the value of **warning** of imminent adversary activity within the homeland security environment, and 2) the value of intelligence as it relates to **anticipating** potential future adversary courses of **action**.

1. Intelligence and Warning in Homeland Security

The decisive test for any intelligence agency is to warn…of trouble before it occurs.

Walter Laqueur (1985, p. 21)

Perhaps the single greatest burden borne by the homeland security intelligence community is that of warning homeland security leaders and practitioners of imminent danger to lives or property. Without the benefit of understanding the intelligence capabilities and limitations of observation (collection) and analysis and dissemination (orientation), homeland security decision makers run the risk of having either unrealistic expectations of "just in time" tactical warnings or perhaps underestimate the extensive value intelligence warning can have at levels below or beyond the national level and within homeland security decision spaces not traditionally considered intelligence consumers.

Intelligence commentator Gregory Treverton (2009, p. 29) suggests this potential frustration is due to the fact that "state and local officials are unfamiliar with the products of national intelligence agencies and are prone to imagine (or hope) that there is magic behind the green door of classification, only the feds would open it." In the opposite, the intelligence community continually asserts they are not in the business of clairvoyance and must rely upon indications (observable activity that can be analyzed for relevance) prior to being able to provide any sort of valuable warning (Magnuson, 2010). The expectation of clairvoyance and omniscience may be the single greatest obstacle to optimizing intelligence within homeland security. Too many homeland security

intelligence consumers seem to expect "the answer" in an environment that not only rules out the certainty of "*the* answer" but obscures the very signals from which "*an* answer" may spring.

2. Mitigate Surprise: Anticipate to Optimize Response

> *Providing warning is the intelligence officer's most difficult task. The devil is partly in the details: it is impossible to preempt a threat without knowledge of the specific plot or plots, and it is almost impossible to unearth all of them.*
>
> James W. Harris (2002, p. 3)

In order to maximize the warning value of intelligence, political psychologist Alex Hybel stresses the need for a paradigm shift away from ***avoiding*** surprises to being able to ***react*** effectively: "There is no sure method for avoiding surprise. But it is possible to minimize surprise by understanding the circumstances under which it might be sought, the variety of obstacles that must be surmounted in order to achieve different surprises and the types of steps that must be taken to overcome such obstacles" (as quoted by Quiggen, 2007, p. 55). With a realistic expectation of the capabilities and limitations of intelligence for purposes of warning, homeland security leaders and practitioners can continually orient their homeland security intelligence efforts and expectations away from ***predicting*** adversary activity within the homeland security environment toward ***observation*** of threat indicators (circumstances, elements, and obstacles) that may *orient* homeland security practitioners and leaders to the impending security threats in such a way as these decision makers are prepared to act or react to adversary activity in the event of engagement.

3. Intelligence and Managing Expectations: Estimates and Predictions

> *History does not encourage potential victims of surprise attack. One can only hope to reduce the severity—to be only partly surprised, to issue clearer warnings, to gain a few days for better preparations and to be more adequately prepared to minimize the damage once a surprise attack occurs.*
>
> Ephraim Kam (1998, p. 223)

No intelligence program in existence today can be said to have a uniform process by which estimations can be generated with enough certainty to be considered "predicted." The problem with security predictions is it is literally impossible to predict the future no matter how much data is obtained or how much human analysis or computation is done (Quiggin, 2007).

The reasons it is impossible to predict the future in a security environment include the issues of constancy of variables and the interplay between variables in an open system (Quiggin, 2007). Chaos theory suggests that similar outcomes can only be predicted in a system where the same variables occur in the same order in the same environment (Kellert, 1993). Because the security environment is an "open" system wherein interact 100s if not 1000s of different operating variables, those few instances where predictions do come to fruition are most likely to be either overly vague as to be of little use to decision makers, or just plain lucky. According to strategic intelligence and security theorist Thomas Quiggin (2007, p. 42), "With only ten different dots to connect, there would be a total of forty-five different dot patterns that could be created. What is stunning, however, is that the ten dots and forty-five patterns can produce 3.47 trillion different outcomes."

Laqueur (1985, p. 42) suggests the impossibility of prediction in a security environment derives from lack of continuity and the limits of extrapolation: "Because prediction is impossible without at least some measure of extrapolation, and because extrapolation does not work without at least some continuity, prediction becomes most difficult when it is needed most—at a time of rapid or radical change."

Time and energy spent attempting to predict homeland security incidents may result in much needed analytical capability wasted, chasing the impossible. Analyst and decision maker time and energy is much better applied to creating an understanding of the threat environment at large and in creating awareness within a decision maker's process that promotes informed and well reasoned solutions to potential problems and solutions before they occur.

4. Summary: The Value of Intelligence in Mitigating Surprise

Surprise…arises in reality from difficulties of comprehension.

Angelo Codevilla (2002, p. 260)

Of all the demands heaped upon the homeland security intelligence community, the greatest in terms of expectation and difficulty may be that of warning homeland security decision makers of imminent threat dispositions. The entire spectrum of homeland security decision makers, from citizens to presidents, expects intelligence to provide advance notice of adversary activities that may challenge homeland security objectives. Warning promotes decision advantage, sound policy decisions and economy of forces and resources much needed for already taxed security efforts. The following pages assert the benefits of intelligence extend beyond just warning but include the value of optimized resources and policy.

B. OPTIMIZE RESOURCES

> *It is precisely when resources are stretched thin and the tasks many, when the forces are evenly matched and the issue trembles in the balance that good intelligence and sensitive interpretation matter most.*
>
> Walter Laqueur (2002)

An appreciation for and skillful use of an adaptive threat orientation may position homeland security decision makers to take advantage of both offensive and defensive security opportunities, "sharpening the gaze" while facilitating a "shortening of the sword" within the execution of homeland security objectives, thus optimizing homeland security efforts by conserving resources and preserving freedoms (Keegan, 2004, p.387). Intelligence, both as a practice and as knowledge, can be instrumental in guiding and shaping economical and appropriate security efforts while promoting tailored and specific focus to policy and tactical decision makers.

1. Intelligence Facilitates Identification of Vulnerabilities and Opportunities

This section is organized around the premise that intelligence-based homeland security decision advantage, associated with resources and policy optimization efforts,

can be most beneficial when used to: 1) mitigate threat significance within security **vulnerabilities,** and 2) optimize efforts to capitalize on security **opportunities** discovered within the threat environment. The value of intelligence in homeland security becomes more demonstrably apparent as decision makers pursue homeland security objectives with limited resources in situations of great potential violence or security consequence.

2. Intelligence-Based Decision Advantage and Homeland Security Vulnerabilities

a. Identifying Vulnerabilities

Vulnerability is a weakness an adversary may seek to exploit (Clark & Chenowetth, 2006, p. 95). As such, vulnerability cannot exist without: 1) a flaw or weakness, and 2) an attacker with the capability and/or intent to exploit that flaw or weakness. Vulnerabilities are not "where we think we are weak" but rather security situations and operational circumstances that intelligence indicates an adversary may successfully exploit.

Intelligence support to vulnerability mitigation efforts includes providing homeland security leaders and practitioners with information that identifies adversary strengths, and weaknesses, intentions, limitations, or any other host of factors that may or may not make a vulnerability more or less worthy or limited homeland security resources. Furthermore, decision makers may derive strategic and tactical benefit from intelligence that is able to determine specific terrorist targeting methodologies, tactics, techniques, and procedures by which they purport to employ. Such threat knowledge can be critical to security efforts geared toward "hardening" potential vulnerabilities against known or anticipated capabilities and also can be invaluable in the creation of strategic plans that address the protection of assets of interest (such as critical infrastructure and key resources).

The validity of vulnerability assessments not based on timely, tailored, and accurate intelligence should be evaluated with tremendous scrutiny. The proximate reality of threat knowledge ought to be the bedrock of every prevention activity because

without a minimum domain awareness of the threat, such knowledge provides, every actor, and every potentially adversarial element is a threat. The U.S. has neither the resources nor the laws or culture to maintain this security posture or engage in potentially uninhibited searches.

C. DEPICT PROXIMATE REALITY

> *The role of most intelligence is not driving decisions in any short term, specific way, but contributing to decision-taker's general enlightenment; intelligence producers are in the business of educating their masters.*
>
> Michael Herman (1993, p. 43)

1. What Is Proximate Reality?

Proximate reality is an illustrative compilation of observations and analysis specific to a certain threat environment at a specific time and place. It is *proximate* inasmuch as it is not, nor can it be, a perfect representation of the "actual" threat, as the dynamic and asymmetric homeland security threat data submit to no such description. The threat description is "reality" in that it is the sum of all the observed and analyzed threat data (signatures, activities, and patterns) analyzed in light of the operational objectives and operating environment within that decision maker's decision space. The value of proximate reality is in the capture, articulation, and sharing of an understanding of a threat environment previously beyond the common experience of a particular decision maker within a specific threatscape.

For the homeland security intelligence analyst or homeland security leader or practitioner, proximate reality may be succinctly defined as a tailored, timely and accurate depiction of the totality of threats observed, analyzed, or anticipated by the intelligence apparatus within the homeland security threatspace.

2. Why Proximate Reality?

> *We use reference points in our heads to start building beliefs around them because less mental effort is needed to compare an idea to a reference point than to evaluate it in the absolute. We cannot work without reference points.*
>
> Nassim Nicholas Taleb (2007, p. 159)

A shared proximate reality can add value to homeland decision makers by becoming a shared "threat narrative" from which they can interweave their own security narratives. Intelligence scholar and RAND research fellow Gregory Treverton (2009, p. 75) suggests:

> Ultimately, intelligence is storytelling. It is helping those who will take action construct and adjust the stories in their head that will guide their decisions. Absent some story, new information about a topic is just factoid. The story provides a pigeonhole and context for the new information.

As a captured and articulated interpretation of a threat, proximate reality has the potential value of cognitively uniting homeland security leaders and practitioners within a common threat envelope on the same threat "page," at least with regards to the capabilities, limitations, and intentions of threats occurring within their shared decision space. Security policy and operations functioning within this shared threat "picture" requiring a collaborative response can then programmatically and uniformly plan, equip, and respond to those threats, potentially economizing resources or mitigating confusion that might have resulted from different decision makers operating from disparate threat "realities." A shared proximate reality creates an opportunity for those exercising judgment within the same sphere of operation to share an understanding of at least the threat reasons for the decisions peers within the same sphere are making.

Lacking an understanding of the proximate reality of a threat environment or situation, decision makers may be left in a reactive state and the unnecessarily vulnerable position of needing to become "spun up" on the threats during a crisis, or run the chance of using dissimilar narratives or experiences as other homeland security decision makers operating within the same threat environment.

3. Intelligence-Based Homeland Security Decision Advantage: Proximate Reality as a Threat Assessment

One purpose of threat assessments is to "bring a policy maker who has never heard of the subject 'up to speed' on the basics of the situation, to project further developments in the area, and to guide the policy maker in the choices that are on the

agenda" (Codevilla, 2002, p. 206). In effect, the threat assessment adds value to homeland security leaders and practitioners because it potentially creates a baseline threat orientation from which changes within that threat environment can be based. Comprehension of proximate reality creates a cognitive space within the homeland security leader or practitioners' minds from threat status dialog and baseline understanding may evolve and develop even as the very threats of consideration evolve and develop. An appreciation for proximate reality of itself suggests the immediate understanding (reality) of the threat is perishable and decisions made based on those realities may of necessity be adjusted as the intelligence-based threat reality changes.

The dynamic and asymmetric nature of the homeland security threat suggests any "proximate reality" will remain "proximate" only as long as the factors by which that reality has been derived remain unchanged. Each time any factor, be it adversarial, environmental, or security driven changes, the "reality" may likewise change. The production and dissemination of "current intelligence" is the process by which intelligence professionals keep decision makers informed of changes as they occur and are observed within the decision space.

Both current intelligence reports and threat assessments are mechanisms of creating or updating proximate reality (both seeking to define the status of adversary capabilities and intent) but due to the limited time and attention of homeland security decision makers, the urgency of current intelligence can run the risk of overshadowing the importance of foundational understanding of a specific or general threat.

4. Intelligence-Based Homeland Security Decision Advantage: Proximate Reality as a Vulnerability Assessment

If security vulnerabilities are "flaws or weaknesses that can be exploited by an attacker," any coherent discussion of vulnerabilities must be based upon knowledge of the attacker (aka capabilities, limitations and intentions) (Jomim, quoted by Rusello, 1991, p. 109). Unsupported and irrelevant vulnerability assessments can result from analysis that does not include timely, accurate, and tailored intelligence. Knowledge of the adversary is paramount for accurate identification, definitions, or descriptions, of

tactics techniques or procedures that may be used to exploit security flaws or weaknesses. Vulnerabilities cannot exist independently from a threat in the same way risk cannot exist independently from vulnerability.

D. THREAT ORIENTED POLICY AND LEGAL DECISIONS

> *Intelligence is a tool needed by policy makers for decisions, a wholly pragmatic enterprise in which results are the only criterion of success.*
>
> Walter Laqueur (1985, p. 293)

Homeland security policy decisions shape how homeland security operations and personnel are organized, trained and equipped. An adaptive threat orientation might then be considered a prerequisite to homeland security policy and legal decision advantage. The role of intelligence in facilitating the acquisition and maintenance of that adaptive orientation and subsequent potential for political and legal decision advantage within that threatscapecannot be overstated. This section will detail and discuss the role of intelligence in acquiring and maintaining political decision advantage from the perspective of federal, state, local, and private industry decision makers.

1. Intelligence-Based Homeland Security Decision Advantage: Political Advantage

> *Intelligence is an asset or a liability depending on whether intelligence helps or hinders the fulfillment of political goals.*
>
> Michael A. Turner (2002, p. 3)

The U.S. Constitution, as the supreme law of the land, calls for a division of not just power within the federal government but between the federal government and the several states (Linder, 2010). The sweeping domain of homeland security encompasses each of these layers and branches of government, none of which can legitimately claim to optimize their security decisions without the application of threat information to their security environment. This section explores the political and judicial benefits of intelligence-based homeland security decision advantage in furtherance of homeland security objectives.

If politics are the confluence and collision of competing interests, then homeland security politics are those with interests rooted in any one of hundreds if not thousands of organizational and personal efforts and initiatives to produce desired homeland security effects (Sullivan, 2009). Contemporary domestic security efforts differ from those of just a generation ago due in part to the rise in threat from global Jihadi extremists and the increased use of terrorism as a domestic form of political influence. Additionally, as the threat of catastrophic terrorist violence has become a reality in the United States, the responsibility for preventing, preparing for and responding to this new threat is shared across nearly every level of federal, state, local, and tribal government. As such, each of these stakeholders comes to the homeland security challenge with distinct charters and desired results (DHS, 2007). Treverton (2009, p. 3) suggests a shift has occurred in potential intelligence consumers, away from only federal or national level leaders, "National intelligence used to be designed primarily for a relatively small set of political and military leaders of states. Now, it could be of use to a huge number or consumers from police officers to private sector managers of major infrastructures."

Distributed government decision-making authority generates competing political interests and potential disparity of access to information (threat and otherwise) among these different decision makers. When governing matters of security, political decision makers would be wise to acquire and maintain an adaptive understanding of threats to that security.

The inclusion of intelligence in the political dialog of homeland security governance adds a depth of understanding necessary to ensure these political decisions are evaluated with the greatest threat understanding possible, lest these security decisions (and subsequent allocation of resources or restrictions of freedoms) be used to pursue interests beyond the scope of security. As such, intelligence clearly has place among all levels and branches of government charged with operating, overseeing (or funding), or enforcing security policy.

2. Intelligence-Based Homeland Security Decision Advantage: Policy Making

Policy leaders determine the utility of the intelligence they receive based on ideological and political factors.

Michael A. Turner (2002, p. 118)

Security policy decisions often manifest as choices of public priorities related to the use of public resources or limiting certain individual freedoms. In the case of homeland security policy, as with similar security policy decisions, "optimal" policy decisions may be considered those decisions that provide the greatest amount of security opportunity with the fewest restrictions or requirements (costs in freedoms or finances) on the constituents or stakeholders whereon security is expected to be provided. Treverton (2001, pp. 178, 185) asserts policy makers rely on intelligence in three stages:

1. If the policymakers are prescient, when the issue is just beginning; however there is likely to be little intelligence on the issue at that point.
2. When the issue is "ripe for decision." Here policymakers want intelligence that permits alternatives to be considered; however, intelligence often is only able to provide background information necessary for understanding the issue.
3. When the policymakers have made up their minds on the issue, but only if intelligence supports their view. They may be uninterested or even hostile when it does not support their view.

This first stage is perhaps the most challenging for the homeland security intelligence analyst to support his or her policy masters, as usually only the faintest signals of threat may be observable, yet, the potential consequences for miscalculating the risk could be severe. The homeland security policy folder is one of many within the docket of state, local, federal, and tribal decision makers when it comes to government priorities. Homeland security leaders and intelligence analysts should be constantly adjusting their threat orientation based on available threat information and risk analysis.

If policy makers fail to orient themselves to a threat prior to a crisis they may find themselves scrambling to "do anything" regardless of the threat or risk.

Former Assistant Secretary of State for Intelligence and Research Morton Abramowitz justifies this dark phenomenon as a result of the uncertainty inherent in security decisions (and policy) as well as a hyper competitive political environment. Since intelligence by its nature deals in uncertainties, Abramowitz confirms the ease of which policymakers "pick the intelligence they like" in the pursuit of political objectives. (Kessler, 2005, p. A5)

Another role of intelligence in support of decision advantage and policy development relates to the limitations of time and attention policy makers can give to an issue. Intelligence commentator and former Senate Select Intelligence Committee staffer Angelo Codevilla notes, “the absorptive capacity of consumers clearly has its limits” and those limits are never less forgiving then during crises (2002, p. 53). If policy makers put off developing a threat orientation until a crisis erupts, at a time when decision makerss should be honing their understanding to a particular threat they may find themselves “drinking from a fire hose” of potential threats or outcomes, in addition to attempting to craft or execute a mitigation strategy. Obtaining and maintaining an understanding of the proximate threat reality therefore may be a critical factor for the beneficial inclusion of intelligence in policy development.

3. Intelligence-based Homeland Security Decision Advantage: Security Functions of American Government

> *The first order of business for US national intelligence…is to inform and warn the President, the Cabinet, the Congress, the Joint Chiefs of Staff and commanders in the field,* ***domestic law enforcement and homeland security authorities*** *in the heartland, and our international allies.*
>
> National Intelligence Strategy (2005, p. 1)

Since 9/11 the federal government has had to reorient its collection and analysis priorities within the United States Intelligence Community inward and rely on state, local, private sector, and citizen threat observations instead of relying exclusively on overseas threat collection to meet the homeland security intelligence requirements (Allen, 2006, p. 3). The attacks of 9/11 awoke the country to the certain fact that the risk of terrorist attacks exists within the boundaries of the 54 states and territories, and that

citizens, state, local, tribal governments, and private enterprise bear a most vital responsibility in observing, analyzing, and disseminating homeland security intelligence to the government that might be crucial in preventing, protecting, and eliminating (by force or prosecution) terrorist threats to the United States.

4. Intelligence-Based Homeland Security Decision Advantage: Federalism and Separations of Powers

The American domestic intelligence and security information sharing experience is unlike that of any other nation because the U.S. Constitution creates separate governance powers and authorities between both the branches of the federal government, and between the "several" states and central federal government (U.S. Constitution, Art I § 2). Because both elected and appointed homeland security leaders and practitioners span the national gamut of government, an unprecedented challenge has arisen in coordinating the appropriate access and usage of intelligence (requirements, analysis, and dissemination) to each homeland security stakeholder in an efficient and effective manner. American Federalism was intended to keep government power from being consolidated in one branch of the government, and is by design, not the most efficient mechanism for governance or information sharing (Metzger, 2003). Federalism does, however, ensure that no one body controls an excessive amount of power, be it legal, financial, or informational. Since responsibilities for addressing security issues are shared throughout and across the government, access to intelligence pertaining to those threats would be wisely shared equally throughout and across the government. This is a critical, if not doctrinal, statutory or Constitutional distinction between homeland security and national security: whereas national security authorities are nested primarily in the Constitutional Article 2 powers of the Executive (and to an arguably lesser extent with Congress), homeland security is a cross-authority, cross-jurisdictional *collaborative* endeavor.

"Power," in the terms of a federalist government, means being able to produce legal consequences by taking action concerning some "matter" (Cornell Legal Institute, 2010). In many matters of national security and many matters of homeland security, the distributions of "legal consequences" (e.g., power) is claimed by the executive branch by

way of Constitutional authority as Commander-in-Chief, as the "sole organ" for international affairs and foreign policy, and his or her duty to "enforce the laws" Congress has drawn concerning terrorism. However, power is also retained by the states in the form of police powers for domestic security matters that do not threaten the "republican form of government" or the good order and execution of federal programs or objectives (Cornell, 2010). These police powers do not arise from the Constitution per se, but are an inherent attribute of the states' territorial sovereignty. From this federalist setting springs the uniquely *national* relationship between security decision makers we have come to call *homeland* security.

a. Security Powers of the State

The Tenth Amendment directs that "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people" (U.S. Constitution, Tenth Amendment). It may then be argued the lion's share of (constitutional) domestic security efforts thus fall upon the states, and not the federal government. Accordingly, under the both statute and U.S. Constitutional law, individual states have both the right and obligation to seek nationally collected and analyzed threat information upon which they can base policies and programs designed to maximize the tranquility and protection of their citizens.

5. Intelligence-Based Homeland Security Decision Advantage: State Police Powers

Police powers are used to regulate behaviors and enforce order within the states' jurisdiction, and are often framed in terms of public welfare, security and safety (Supreme Court Center, 2009). Included in the police powers of the state are those powers under a state's constitutions that provide for the implementation of martial law or other increasingly restrictive government mechanisms used to address homeland security incidents. Security actions taken by the state that may infringe upon the liberty of citizens ought to be considered as so serious as to demand the inclusion of the very timeliest, tailored and accurate intelligence available.

Since "all homeland security incidents are local" and elected officials and state and local leaders are responsible for the immediate security of their communities, threat information pertinent to the security of the states and communities ought to be considered in the planning, programming (budget), and training necessary to address those objectives (White House, 2003). Not every state or community may want, need, or be able to afford instant or constant intelligence feeds from national or regional intelligence producers. Intelligence needs will likely be as diverse as the level and scope of authority and responsibility of the homeland security leaders and practitioners involved. Some organizations may desire to develop their own observation and orientation programs instead of relying on the national system in place. Some state and local organizations have even gone as far as to create their own overseas collection and analysis services, effectively "working around" the United States Intelligence Community (USIC) for source intelligence deemed critical for homeland security decision makers "back home" (Viana, 2008).

Many state constitutions provide mechanisms for Governors to engage in security practices that dramatically reduce personal freedoms during time of crisis (Lowenberg, 2010). The value of intelligence for state and local homeland security leaders may be at its greatest when governing the balance of the needs of liberty and security at the lowest and most personal levels.

6. Intelligence-Based Homeland Security Decision Advantage: Security Functions of the Federal Government

a. The Executive Branch

Under the Constitution, the President assumes Constitutional and statutory national security authority under the "Commander-in-Chief" powers as well as the "laws enforced" powers (U.S. Constitution, Art. II §2). The President also *shares* emergency powers with the Congress, the Judiciary, and the American people (in the states) under Article IV § four, which directs the whole of government "provide for the common defense"(U.S. Constitution, Art. IV, §4). Additional support for the role of the executive in homeland security can be found in the actual language of the Constitution, which

requires the executive "take care" when executing the laws of the nation; this taking "care" with regard to executive governance within a threat decision space most certainly includes the responsibility of acquiring and maintaining an adaptive threat orientation (U.S. Constitution, Art. II §2).

The security role of the executive has arguably increased in presidential priority since September 11, 2001 (Justia.com, 2010). Columbia University Law professor and Constitutional scholar Henry P. Monaghan (1970, p. 25) has proposed that contemporary Presidents have embraced the role of "Protector-in-Chief" and with "ever-increasing frequency…employed that amount of force they deemed necessary to accomplish their…(security) policy objectives." As the executive's assumption of domestic emergency powers has increased, by extension so has the federal demand for the production of domestic intelligence and foreign intelligence with the potential to impact the homeland security environment.

7. Intelligence-Based Homeland Security Decision Advantage: Executive Homeland Security Policy

Modern executive level policy specific to homeland security and counterterrorism efforts began in 1986 with President Ronald Reagan's issue of a *National Security Decision Directive* after the hijacking of the Achille Lauro directing the State Department to coordinate federal international terrorism policy (White House, 1982). Twelve years later President Bill Clinton (1994) issued the *Five Year Interagency Counterterrorism and Technology Plan*, through the Justice Department, seemingly shifting the focus away from the State Department and diplomatic solutions toward a law enforcement focus. After 9/11, an avalanche of presidential guidance was generated in an effort to focus the national, but especially federal, response to the "global war on terror," arguably shifting

(or at least sharing) federal focus towards the Department of Defense prior to the creation of the Department of Homeland Security.[1]

While only Executive Order 12333 is central to intelligence, all of these documents reference specifically, or by extension, the critical value of intelligence in the creation or execution of homeland security operations. These policies articulate the executive's priorities and attempt to establish a cohesive approach to the exercise of government resources and attention with regard to intelligence driven and risk based homeland security actions. In addition to strategies and planning documents, the Executive branch publishes higher fidelity guidance with regard to homeland security in the form of *Homeland Security Presidential Directives*. Unlike strategies, these directives are functional as executive orders and carry the full weight of federal law (Moss, 2000).

While Executive sponsored strategies do not carry the weight of law these policies act to provide a framework from which other executive branch agencies can draft their policies. These policies likewise inform and invite state and local governments, and private actors to plan and operate collectively within a national framework.

Under the *National Emergencies Act*, the President may exercise power only after declaring a "national emergency" (50 U.S.C 1601-1651, 2009). No statutory definition exists however for a "national emergency," therefore it is a political, not exclusively legal decision to declare such an event. The luster of intelligence can support the President's decision to declare an emergency. Executive power can also be extended by invoking the Stafford Act, which permits the President to provide federal assistance to states requesting assistance on the basis of insufficient state resources or expertise in performing relief efforts (Robert T. Stafford Disaster Relief and Emergency Assistance

[1] The *National Strategy for Homeland Security* is the overarching executive policy for both the Department of Homeland Security and national homeland security efforts. Subordinate or companion policies (White House) include: National Security Strategy of the United States of America (2002), National Strategy for Homeland Security (White House, 2002), National Strategy for Combating Terrorism (2003), National Military Strategic Plan for the War on Terrorism (2002), National Strategy to Combat Weapons of Mass Destruction (2002), National Money Laundering Strategy (2002), National Strategy to Secure Cyberspace (2002), National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003), and National Drug Control Strategy (2002).

Act, 1998). When emergencies where the "subject area" is "exclusively or preeminently in the federal purview" the President does not require a request from the State governor to invoke the Act and deploy federal, to include Department of Defense, resources to the affected area (Robert T. Stafford Disaster Relief and Emergency Assistance Act, 1998). Again, this is a political decision that might seek to borrow weight and imply **justification** from the use of intelligence.

8. Intelligence-Based Homeland Security Decision Advantage: The Executive Cabinet

Homeland security (and asserted by extension intelligence) statutorily "touches" no less than 12 of 15 Cabinet Secretaries (Secretaries of State, Defense, Homeland Security, Energy, Health and Human Services, Transportation, Labor, Commerce, Agriculture, Interior, and the Attorney General). Additionally each state and territory relies on its police powers to protect its citizens and a constitutionally protected right to defend against "invasions." The Constitution continues, "the powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people**"** (U.S. Constitution Art I, U.S. Constitution, 10th Amendment). An examination of the responsibilities and objectives of the two most significant "consumers" of State, local, and private sector information is illustrative as to why these agencies request access to such information and intelligence.

9. Intelligence-Based Homeland Security Decision Advantage: Department of Homeland Security

By statute (6 U.S.C. §111(b)(1)(a-h), 2004) the Department of Homeland Security's (DHS) mission is to:

> (A) prevent terrorist attacks within the United States;
>
> (B) reduce the vulnerability of the United States to terrorism;
>
> (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;

> (D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;
>
> (E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;
>
> (F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland; and
>
> (G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

DHS is legally prohibited from "investigating and prosecuting acts of terrorism" with this authority reserved for "Federal, State, and local law enforcement agencies with jurisdiction over the acts in question" (Homeland Security Act 2002, Pub. L. No. 107-296, 116 Stat. 2135. With the exception of the Secret Service, Immigration and Customs Enforcement, and the Coast Guard, DHS is completely divorced from investigative and law enforcement functions particular to the Department of Justice. Thus the foremost information sharing and intelligence objectives of DHS is prevention of terrorist acts not criminal prosecution (Homeland Security Act 2002, Pub. L. No. 107-296, §111).

DHS (HSA 2002, 102(C)(3)) also has by law, the obligation of "distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public." It is with this charge that DHS seeks to "fuse" information derived from national intelligence sources with locally provided information and intelligence purportedly creating a comprehensive threat picture based on all available information.

a. Department of Homeland Security Information and Analysis Division

The Department of Homeland Security Information and Analysis (DHS I&A) division exists to "identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely

warnings, and immediately take or effect appropriate preventive and protective action" (White House, 2010). DHS I&A has two primary responsibilities: 1) Threat analysis and warning, and 2) Critical infrastructure protection.

b. DHS Threat Analysis and Warning

The DHS threat analysis and warning mission is accomplished by analyzing threat information gathered by the law enforcement, defense, and "all source" information from such varied contributors as public health and weather. DHS I&A is responsible for the national Homeland Security Threat Advisory system and national alerts. Since a purported 85 percen of the nation's critical infrastructure and key assets are within the private sector a critical government mechanism for informing private sector leaders responsible for security of those assets and systems is the DHS Homeland Security Operations Center (HSOC) (Bellavita, 2009). The HSOC collects, fuses, analyzes and disseminates intelligence reports on industry specific issues and issues specific warnings and intelligence to the private sector in those potentially affected areas (DHS, 2008).

c. DHS Critical Infrastructure Protection

The Office of Information Analysis and Infrastructure Protection (I&A) is a statutorily mandated division of the Department of Homeland Security with sweeping intelligence and threat analysis responsibilities including the statutory obligation to:

1. Access, receive, and analyze all source data relating to homeland security interests from Federal, State, local agencies (including law enforcement), private sector entities, and integrate that information in support of Department of Homeland Security missions;
2. Carry out comprehensive threat assessments on the vulnerabilities of key resources and critical infrastructure of the United States;
3. Integrate the relevant threat information and vulnerability assessments in order to identify priorities for protective support measures;
4. Ensure the timely and efficient access to all information needed by the Department of Homeland Security to accomplish its missions;
5. Develop a comprehensive national plan to secure critical infrastructure and key resources;

6. Recommend measures necessary to protect critical infrastructure and key resources in cooperation with the State, local, Federal and the private sector;

7. Disseminate information analyzed by the Office of I&A throughout the Department of Homeland Security and all other Federal, State, local, and private sector agencies, organizations, or individuals with responsibilities relating to homeland security;

8. And to consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information relating to threats of terrorism against the United States;

9. Ensure all intelligence and information is protected from unlawful disclosure and shared, retained and disseminated consistent with published national standards; request additional information from other agencies of the federal government, State and local government agencies, and the private sector relating to threats of terrorism or other areas of responsibility assigned to the Secretary of the Department of Homeland Security (Homeland Security Act 2002, Pub. L. No. 107-296, §121(d)(1-10)).

These comprehensive (and statutorily required) responsibilities are testament to the colossal expectations the nation has of the intelligence function of the Department of Homeland Security.

The DHS Office of I&A is also required by law to request both information from, *and* disseminate intelligence to non-federal organizations (state, local, and private sector entities) **without** the borrowed subpoena power of the Justice Department to compel disclosure. As such, I&A must rely on non-coercive means to acquire the information and intelligence it requires to accomplish its mandated missions. DHS I&A must also rely on the domestic threat observation and orientation contributions of United States Intelligence Community (USIC) collectors, such as the Central Intelligence Agency, the National Security Agency, the National Geospatial Agency, the Defense Intelligence Agency, and the State Department's Office of Information and Research for overseas threat indicators or signatures. For domestic collection DHS I&A relies on its organic intelligence collection through the agencies it controls (Customs and

Border Patrol, Immigration Customs Enforcement, Secret Service, Coast Guard, and the Transportation Security Agency) in addition to information collected from state, local, private sector, and the general public.

10. Intelligence-Based Homeland Security Decision Advantage: Federal Bureau of Investigations

In the United States, domestic intelligence collection is politically and largely culturally regarded as a task for law enforcement (Dycus et al., 2002, p. 431). The Attorney General of the United States is expressly vested by Congress with "primary investigative authority for all Federal crimes of terrorism" (18 U.S.C. §2333b(f)). Within the federal government, by current policy, the National Security Branch (NSB) of the Federal Bureau of Investigations (FBI) has the broad legal authority to collect domestic intelligence within the United States (FBI, 2010). Although the FBI has no legislative charter to conduct intelligence operations per se, it operates under the Attorney General's authority to appoint officials to:

> …detect and prosecute crimes against the United States, assist in the protection of the person of the President; and to conduct other investigations regarding official matters under the control of the Department of Justice and Department of State as may be directed by the Attorney General (28 U.S.C. §533).

On the topic of domestic intelligence operations, a key legal distinction that deserves note is the perceived difference between intelligence operations (collection, analysis, and dissemination) for *prevention* purposes and intelligence operations for *prosecution* purposes. Three levels of federal interest arise in the execution of domestic national security intelligence operations: 1) threat assessments, 2) preliminary investigations, and 3) full investigations (Office of the Attorney General, 2003, p. 5). Understanding the "level" of investigation is important for the government, citizens, and stakeholders as the "level" drives different degrees of scrutiny and access to information gained during the process.

Homeland security leaders and practitioners seek intelligence to orient themselves to the threat within their jurisdictional or topical environment and decision space. What

homeland security leaders and practitioners need is information to help them make better decisions, not necessarily more concrete criminal cases. Not every decision space in homeland security is law enforcement specific, yet an overwhelming amount, perhaps even the "default setting" for homeland security intelligence is law enforcement information. Much of the information needed to create the desired threat orientation lies beyond the suspicion of crime and within the databases of many private sector enterprises (O'Harrow, 2008). Examples of desired information may include information about individuals (travel, commercial transactions, familiar associations, religious affiliation etc.,) transportation, finance, health, and critical infrastructure.

11. Intelligence-Based Homeland Security Decision Advantage: Other Federal Agencies

The value of intelligence at the Central Intelligence Agency is irrefutable as it has the responsibility of the "coordination of the collection of national intelligence outside the United States though human sources," and therefore can only conduct national intelligence collection within the United States by non-human intelligence means (Intelligence Reform Act §1011, 50 U.S.C.A. §403-4a(d)(3). It is culturally accepted but not statutorily required that the CIA will restrain domestic intelligence collection efforts to technical collection (cyber) and open source collection with an international intelligence or counterintelligence nexus (Fisher, 2007).

Other federal agencies that may request homeland security intelligence are the Environmental Protection Agency (Lee, 2003), the Department of Defense (2008), the Department of Health and Human Services, (2010), the Department of Energy (2010) and the Department of the Treasury (2010) or any other federal agency as directed by the President (White House, 2005).

12. Intelligence-Based Homeland Security Decision Advantage: Congress

The Constitution grants the Congress power to "make all laws that will be necessary and proper" for the function of the federal government (*United States Constitution* Art II, § 8). Since 1947, Congress has passed over 17 Acts specific to intelligence and another 15 acts with domestic security implications. In addition to its

lawmaking powers, Congress has broad financial powers to provide for the "common defense" and "general welfare" of the United States, both of great influence in matters of homeland security and information sharing and intelligence (U.S. Constitution, Art. 1§ 8, (1).

By proportion of words, the constitution gives an overwhelming amount of authority for national security to Congress. Article I powers (Congressional) trump "two-to-one" the named national security authorities given in Article II (Executive) that may gain benefit from the threat orientation intelligence can facilitate, and include the responsibility to:

- Declare war
    - Some role of Congress in the commitment of troops to combat
- Raise and support the armed forces
- Make rules for the government and regulation of land and naval forces
- Regulate commerce with foreign nations
- Provide for the militia and for calling it forth to execute the laws of the Union, suppress insurrections, and repel invasions
- Make all laws that shall be necessary and proper for executing any power conferred by the constitution
- Provide for the common defense (fund) (*United States Constitution* Art II, § 8 Id. Sections 1-10)

13. Intelligence-Based Homeland Security Decision Advantage: Lawmaking

The era of congressionally authorized statutes governing intelligence began with the National Security Act of 1947. Since 1947 Congress has been a vocal critic, quiet consumer and significant influence within the intelligence community. After 9/11 congressional response by way of new and revised statutes was both swift and voluminous. The most significant post-9/11 statutes include:

- *The Intelligence Reform and Terrorism Act of 2004*
- *The Homeland Security Act of 2002*
- *The USA Patriot Act of 2001*
- *USA PATRIOT Improvement and Reauthorization Act of 2005*

- *The Military Commissions Act 2006*
- *The Aviation and Transportation Act of 2001*
- *The Border Security and Visa Reform Act of 2002*
- *The Maritime Transportation Act of 2001*
- *The Public Health Security and Bioterrorism Preparedness and Response Act of 2002*
- *The Terrorism Risk Insurance Coverage Act of 2002*
- *The Terrorist Bombings Convention Implementation Act of 2002*

14. Intelligence-Based Homeland Security Decision Advantage: Additional Congressional Homeland Security Objectives

In addition to lawmaking and appropriations, the Congress is instrumental in maintaining balance of power within the federal government by use of its oversight authority. Congress exercises this authority by reviewing, monitoring, and supervising federal agencies, programs, activities, and policy implementation by way of standing committees and ad hoc hearings.

The relationship between the intelligence community as an appendage of the executive branch and Congress as a consumer or overseer has perhaps a much a tumultuous history as can be had between a functions of government under executive power (intelligence) and another branch of government (Snider, 1997). Politically, Congress has a penchant for "throwing" intelligence "under the bus" for failures of government involving security interests or for overstepping the legal or policy bounds the intelligence agency was directed to abide (*Pelosi vs CIA*, 2009). The intelligence community likewise has from time to time expressed exasperation at being caught between the security policy machinations of the executive and his Cabinet and the desires and intents of Congress (Shelby, 2002). A common, yet key, meme for intelligence professionals with regard to "the Hill" is that Congressional committees with intelligence stewardships are often less interested in overseeing and supporting improved intelligence than fixing blame and finding fault for political reasons (Tenet, 1995).

15. Intelligence-Based Homeland Security Decision Advantage: The Judiciary

A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information.

Chief Justice John Marshall, (Supreme Court decision Tatum v. Laird, 1971)

The judicial branch is charged with interpreting the laws Congress enacts and ruling on the constitutionality of executive actions (Onecle, 2005). Admittedly, intelligence is not evidently critical for the good order and function of the judiciary, however in the application of the law an understanding of incident circumstances and threats at the time of an act may be beneficial in determining the "reasonableness" of actions taken within the homeland security threat environment in determining matters of law.

16. Intelligence-Based Homeland Security Decision Advantage: At Common Law

In addition to Constitutional law and statutes and regulations, the courts rely on common law rulings to guide judicial interpretation of homeland security law. Common law is derived from judicial decisions and opinions that are constantly evolving as new cases and rulings emerge (Blacks, 1999). Common law has legal implications for intelligence and information sharing because of the civil lawsuits that could potentially emerge as a result of negligence and complicated contracts. The effect of intelligence on common law is perhaps most likely to affect the following fundamentally accepted legal principles:

a. Negligence

Intelligence can have a decisive role in determining homeland security negligence rulings because the legal standards for negligence claim take account of a "failure to exercise the standard of care that a reasonably prudent person would have exercised in a similar situation," (Blacks, 1999, p. 1056) or as "conduct that falls below the standard established by law for the protection of others against unreasonable risk of harm" (Law.com, 2010). Without even a perfunctory understanding of the potential

threat, defining the elements of a standard of reasonableness or appropriate "standards of care" may prove excessively cumbersome for judges and juries to uniformly establish. Prior to 9/11 the duty of care and reasonableness factors did not reach or include elements common to terrorism. As of yet, even in the wake of 9/11, the courts have yet to formalize, a new "reasonable person" standard for terrorism cases but numerous legal scholars suggest the sensational nature and prevailing fear that "terrorism can strike anywhere" will in fact force a reconsideration of reasonableness elements of counter terrorism and security standards (Findlaw.com, 2010).

b. Contracts

A contract is an agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law (Blacks, 1999, 2131). With regard to homeland security cases, common law actions for breach will likely involve one party defaulting or seeking to terminate as a result of a potential or actual homeland security incident (Anikeef, Bethune, Gage, Housman, Kalberman, Krachman et al., 2003, p. 78). Whether direct or tenuous, parties may seek to apply either a force majeure (Mitras, 2008, p. 350) or frustration (Black's, 1999, p. 679) legal defense to contracts lawsuits. An appropriate understanding of the situation via an accurate threat orientation could be vital in determining issues of fact and reasonableness in contracts cases.

17. Intelligence-Based Homeland Security Decision Advantage: The Statutory Role of Intelligence

> *Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies* ***must act in partnership*** *to* ***maximize the benefits of information gathering and analysis*** *[emphasis added]to prevent and respond to terrorist attacks.*
>
> 6 U.S.C § 48 (b) 10

A very good reason to acquire and apply threat knowledge in a homeland security decision-making process is in many cases, it is statutorily required—that is, it is the law. Intelligence law dictates how intelligence collection, analysis, and application efforts must be conducted, in addition to influencing other significant legal doctrines (like torts

and contracts) within the homeland security realm. Most homeland security laws are federal in nature, and thus apply primarily to the federal government, however recent case law exists that suggests failure to comply with any reasonable procedures that could have avoided "disruptions" or injuries may be considered as "strong evidence of actionable negligence as a matter of law" (Connecticut State Supreme Court, 2006).

E. OVERCOME DETRIMENTAL PSYCHOLOGICAL AND DECISION BIASES

> *The human mind is poorly designed to deal with uncertainty and so tends to seek information that confirms an already-held judgment and rejects information that is contrary to the prevailing view.*
>
> Richard J. Heur (1999)

1. The Priority Value of Intelligence in Making Decisions

Decision scientists and information management theorists assert that information has non-linear instead of linear value (Foster, 2005). Knowledge of an adversary's capabilities, limitations, and intentions literally define the environment as one requiring security efforts in the first place. Without any foreknowledge of the "boogieman" there is neither reason to fear nor take security precautions to protect against that threat.

For example, if in attempting to thwart imminent terrorist attacks, information regarding the capabilities and limitations of a terrorist group may have greater tactical value than the ideology or history of that group. Similarly, information regarding specific terrorist group leadership profiles may have less value to an elected official voting on homeland security budget issues than information regarding the strategic terrorist partnerships or state ties a terrorist organization may maintain.

Two factors that may drive a heightened psychological value of intelligence for homeland security decision makers are the analytical characterizations of information based on 1) timing, and 2) relevance (Klein, 2003). This is important for homeland security decision makers seeking threat understanding because "racking and stacking" information under extreme psychological stress without being oriented to the potential security impact certain different types of information can have on decisions could result in ill-advised decisions with potentially (yet avoidable) catastrophic consequences.

2. Intelligence-Based Homeland Security Decision Advantage: Overcoming Decision Biases

> *Biases are preferences or tendencies that can undermine rigorous analytical inquiry by influencing or predetermining our approach and its outcomes.*
>
> Gary Klein (IAD, 2009, slide 53)

The importance decision makers place on previous cognitive understanding as a mechanism for considering new decisions is critical according to decision science research professor David Snowden (2007, p. 220):

> What we actually do is search our memories to find the pattern from our previous experiences that appears to fit. If we cannot find a pattern from our previous experiences then we extrapolate possible future patterns until the first 'fit' one appears to apply and use that.

As homeland security proximate realities ought to change in direct relation to the rate of threat change (and the ability of intelligence to observe and orient in relation to that change) and environmental change, each "former" reality then may become a "previous experience" per Snowden's decision-making model.

Homeland security leaders and practitioners who disregard the potential negative impact of decision biases may run the risk of marginalizing the importance of new information or ideas and thus undermine their own decision advantage. The inclusion of intelligence into the decision process can assist decision makers to identify and overcome such biases, as doing so can facilitate the creation of new cognition and narratives, or provide evidence that biases and heuristics currently embraced are unsupported by fact or theory. The following is a synopsis of psychological biases, the negative effects of which may be avoided or mitigated if threat intelligence is included as a decision factor. Additionally, although not a bias per se, certain heuristics can be confronted and challenged by using an adaptive threat orientation (Croskerry, 2002).

a. Vulnerability Heuristic

A heuristic is a mental shortcut or pre-selection decision makers may rely upon to order situations into familiar mental processes (Everson & Hammer, 2010). A

popular, yet potentially limiting heuristic within the homeland security community is the *vulnerability* heuristic; which suggests when threat knowledge (capability, limitation, intent) is absent, uncertain, or unknown then risk models should be based strictly on widely accepted but un-validated security vulnerabilities within the system in question (Delor & Hubert, 2000). This heuristic is limiting because it effectively reduces the impact value of the threat quotient within the risk formula, potentially dramatically skewing the results, generally in favor of increased resources to "shore up" the vulnerability while adding little if any true risk protection.

The Government Accounting Office (GAO, 2000, p. 6) reports on the potential drawbacks of the vulnerability heuristic:

> Without the benefits that a threat and risk assessment provides, many agencies have been relying on worst case scenarios to generate countermeasures or establish their programs. Worst case scenarios are extreme situations and, as such, may be out of balance with the threat. By using worst case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited). By targeting investments based on worst case scenarios, the government may be over funding some initiatives and programs and underfunding the more likely threats the country will face.

An adaptive threat orientation focuses the threat into the context of the decision maker's goals with regard to securing both the vulnerability and the greater security within the decision space. In an environment of limited resources, vulnerability heuristics can handicap decision maker's efforts to prioritize time or available resources in furtherance of their security objectives.

b. Choice Biases

A bias is a term used to describe a tendency or preference towards a particular perspective, ideology or result, when the tendency interferes with the ability to be impartial, unprejudiced, or objective (Dictionary.com, 2010). Cognitive biases, or biases related to a person's tendency to make errors of judgment based on processing of information, may be particularly troublesome for homeland security practitioners and leaders who, perhaps without foundational understanding of threat situation, thrown into

situations of extreme volatility without knowing either the proximate reality of the threat situation or the capabilities and limitations of intelligence to know and communicate such understanding (Allpsyche, 2010). The remainder of this chapter focuses on identifying and acknowledging the existence and impact these biases can have on homeland security decisions and how intelligence might be a useful enabler in overcoming these biases.

1.) Habit. Familiar options are often the first sought by decision makerss because they are usually deemed reliable (Lowenstein, Donoghue & Rabin, 2003). The asymmetric nature of homeland security threats and the unique response usually required to prevent, protect, or respond to threats to domestic security very likely will require unfamiliar, or at least less commonly relied upon responses. Threat information can cue decision makerss to consider options other than the most familiar.

2.) Attenuation: Oftentimes decision makers will attempt to simplify or categorize a situation into a preexisting solution set (Jenkin, 2006). Timely and accurate application of threat information can help to avoid the undue simplification of complex situations and the unintended consequences of "low-balling" the potential outcome of a situation.

c. Confidence Bias

1.) Completeness Bias. Once a certain degree of confidence is attained, the temptation can arise to not only cease to consider alternative outcomes or solutions, but deliberately seek to quell such dialog. (Sulistyawati & Chui, 2009). Intelligence can be a valuable asset when attempting to keep decision makers oriented to the threat situation as the observations and analysis indicate and not by faulty assumptions or outdated confidences interpret them to be.

Additionally, improper use of intelligence or disregard for an adaptive threat orientation can fuel completeness bias in that decision makers may cling to decisions previously made based on intelligence presented at the time that may have since changed. Reliance on "the answer" in lieu of "an answer" based on the best available threat intelligence may be indicative of completeness bias and may result in suboptimal or unnecessarily rigid security decisions or courses of action.

2.) Confirmation Bias. As opinions, courses of action, or concepts of reality are created, the occasion may arise that may promote a selective focus on only new information that confirms the decision makers' view, often ignoring or rejecting contrary data (Nickerson, 1998). Intelligence is generally (or at least theoretically should be) distinguishable as from other information relied upon by to decision makers as being derived from the observation and analysis of events outside of the direct influence of that decision maker, and thus (theoretically) insulated from confirmation biases. Intelligence professionals have an obligation to convey both the threat knowledge available and the potential consequences that could accompany rejecting or ignoring such knowledge.

3.) Memory Biases. Selective recall is an example of a memory bias by which the disproportionate use of information we remember and/or use, primarily because of how recent or prominent in the memory due to emotional content the information is (Roy, Christenfeld, McKenzie, 2005). Threat knowledge can be especially valuable in overcoming memory biases because of the extreme emotional response to homeland security threats and events.

4.) Naïve Statistics Biases: Frequencies and Probabilities. According to research, decision makers have a tendency of erroneously correlating frequencies and probabilities (Reyna, Brainerd, 2008). Intelligence can assist homeland security decision makers understand the spectrum of possible events or courses of action holistically, without relying strictly on single source statistics or probabilities.

5.) Adjustment Biases: Anchoring and Conservatism. The assessment of departures from an expected norm ("unusualness") is generally unduly influenced by the assessor's baseline expectation (Bunn, 1975). The reluctance to change mental models in the face of unexpected or undesired information is consistent with conservatism. Threat knowledge can help to expose decision makers both to the threat behavior departures observed and the potential consequences of inaction in favor of conservative bias.

6.) Presentation Biases: During a crisis, eye-watering amounts of information can be presented to decision makers, often framed in the perspective of the individual or agency presenting the information. A uniform, or at least cursory understanding of the threat the organization or coalition of organizations face (as is usually the case in homeland security events) can be helpful in creating a common threat "frame" from which potential courses of action can be created, and from which departures from that frame can be scrutinized and accepted or rejected.

7.) FalseA. The cognitive adaptive theory of problem solving suggests we address problems by drawing upon solutions to problems we have faced in the past and applying those solutions (with adaptations as necessary) to current challenges (Gentner & Landers, 1985). Tailored, timely, and accurate threat information applied, (understanding) can be used by decision makerss and their staffs to challenge analogies and avoid the drawing of analogies that are inconsistent with the existing threat situation.

8.) Attribution Biases. Information can be over-credited or discredited based on its attribution (source) (Tetlock & Levi, 1982). Furthermore, attribution in a social psychology decision-making model suggests an attribution risk exists when decision makerss attribute the cause of events or behaviors to personal or group characteristics rather than circumstances (Id). The importance of attribution is no small factor in investigating or responding to homeland security events, thus timely and accurate threat information regarding the event can be critical in overcoming potential decision-based attribution errors.

3. Summary

Intelligence can be valuable in overcoming psychological barriers to effective decision making because:

- The relevance and impact of intelligence in contrast to other types of information in a security environment may lubricate choice with regard to potential courses of action based on known or anticipated consequences

- Intelligence can temper fear of the unknown or the unknowable by distinguishing that which is known and can be knowable from that which is not or cannot be known or knowable
- Intelligence can be valuable in overcoming heuristics and biases detrimental to effective decision making because it can facilitate the creation of new and more accurate cognition or narratives, or provide evidence that biases and heuristics currently embraced are unsupported by fact or theory

F. INTELLIGENCE-BASED HOMELAND SECURITY DECISION ADVANTAGE: INTELLIGENCE AS A COMMODITY AND SYMBOL

Intelligence can be valuable to homeland security leaders and practitioners as a status symbol or as a commodity in and of itself. Not an "operational" value per-se, the commodity and symbolic value of intelligence can be used as leverage to further both organizational and personal objectives. The decision advantage that intelligence can provide can add to the reputation of a decision maker. One known to have access to intelligence can be seen by others without that threat understanding or access as having either access or information advantages.

a. Intelligence as a Commodity

Economists establish the value of a product or service may be calculated by determining either 1) its exchange value or 2) its operational value (Demming, 1999). The *exchange* value of intelligence may be driven by how much an organization or party is willing to compensate (in barter or cash) for access to or possession of that intelligence. During the Cold War the intelligence collection focus of the U.S. government was foreign, not domestic. The idea of having to pay for or barter for intelligence, data, or information is relatively new within the federal U.S. intelligence community at large, as until 9/11 they had a monopsony (a buyer's monopoly) on all nationally relevant intelligence. All of the intelligence needed for pre-9/11 federal security actions were deemed to be the purview of the federal government (with the Federal Bureau of Investigations handling domestic security intelligence). In a post-9/11 era, with much of the intelligence collection and consumption needed for homeland security decisions being centered in the sub-national and private sector level, a new paradigm for domestic

collection and consumption must be adopted giving "owners" of intelligence data or information of interest to the government an exchange value from which they can operate. Homeland security leaders and practitioners that possess this desired information may be in a position to leverage this exchange value within the homeland security intelligence community or with other homeland security decision makers for political, organizational, or information advantage.

b. Intelligence as a Credential

Another tangible benefit of participation within the intelligence community is the much coveted "blue badge" or security clearance that entreats one access behind the secrecy "curtains" drawn to keep intelligence sources and methods secure. While the whole matter of security clearances for homeland security leaders and practitioners is a hotly debated issue within the homeland security community, the fact remains leaders and practitioners with security clearances are granted greater access, and are subsequently more privileged to information and classified peer networks than those that do not have a security clearance. There is also the perception of a heightened status or professional reputation among the popular media also often chooses to identify domestic public safety personnel as either having a security clearance or not, again signifying the heightened status of one having access to information others do not (Reese, 2005).

2. Conclusion: Why Is Homeland Security Intelligence So Hard?

I don't know what kind of intelligence I need but I know it when I get it.

Henry Kissinger (1981, p. 252)

Due to the distributed accountability for domestic security decisions spread throughout the country and across the political spectrum, leaders and practitioners that were not previously able to or required to rely on national level intelligence agencies for knowledge are now having high level intelligence thrust upon them, very often with little or no orientation or understanding of what that intelligence has to do with their decisions. With such a wide, deep and diverse pool of potential decision makers, those responsible for homeland security intelligence production and orientation are woefully under-

resourced and under-networked to do the orienting for which they should be charged. The threat information required by a city council to make security decisions related to a municipal budget is much different than the threat information required by the Joint-Terrorism-Task Force to interdict or disrupt terrorist activities. But in many cases homeland security decision makers are relying on the same processes and products to provide observation and orientation for both decision-making bodies. Homeland security intelligence is difficult in part because of the enormous quantity of homeland security leaders across the nation demanding timely, tailored, and accurate threat information.

Perhaps one of the most formidable challenges to heightened threat understanding within the homeland security community are unreal expectations of what threat information can uniformly provide and what it cannot. In an age of dramatic Hollywood and television espionage thrillers, homeland security consumers run the risk of becoming unrealistically reliant upon "just in time" predictive assessments where intelligence analysts are able to pinpoint the location of terrorist suspects or threatening devices based on mythical satellite capabilities or one-in-a-million analytical connections.

Intelligence represents a programmed and repeatable transition of data from secrecy and ignorance to openness and utility, the ultimate benefit of which should be the decision maker's increased understanding of a threat. At the apex of its value intelligence can be a comprehensive, reliable, swift, and relevant mechanism by which decision makers can observe and orient their own decisions in light of the challenges brought on by various threats to organizational objectives.

G. SUMMARY

- The aggregate value of intelligence to homeland security decision makers can be deduced as decision advantage within decision spaces occupied by a threat. If there is an ideal "end state" for HSINT, it may be as a facilitating factor of decision advantage, an advantage that requires constant observation and orientation to the ever-changing threat capabilities, limitations, and intentions within the homeland security environment.
- Homeland security leaders and practitioners should fund, organize, equip, train, and rely on intelligence for two primary operational purposes—to mitigate the negative effects of surprise and to optimize security efforts.

These are the "fruits" of the intelligence labor by which all operational intelligence support should be evaluated. Both of these "fruits" however stem from the tree of threat understanding, defined in this chapter as the depiction of proximate threat reality.

- If not for the uncertainty inherent to the homeland security environment, the costs in resources and potential limitation of liberties required by intelligence may be difficult to justify. This chapter seeks to define and examine the specific values of intelligence as a "tempering" agent.

At best, the intelligence support homeland security leaders and practitioners, elected officials, leaders of industry and service organizations, the media and especially the American people can expect to reliably and consistently receive is in direct proportion to the amount of collective priority intelligence receives in the development of policy and execution of security operations. It is unreasonable to expect to be immediately oriented to a complex threat environment that has vexed the security community of the world for the past 100 years merely because it effects them now. Leaders and practitioners willing to pay the price in treasure and attention to attain and maintain an adaptive threat orientation will be more adequately postured to operate in this threat environment than those that do not. Decision advantage against a globally connected, highly adaptive and ruthless enemy, whose identities, targets, and modus operandi can change literally at the speed of thought is a most audacious goal for homeland security decision makers and one we should pursue, knowing full well we may fail more times than we succeed, but that even in the attempt to secure decision advantage we will reach a level of threat understanding across the homeland security enterprise previously unattainable.

Of all the fruits of intelligence for the picking, I submit the greatest is threat ***orientation***. Good intelligence may be written, posted or spoken, but as I have outlined here, any intelligence can be of great importance or no importance depending on the use to which the recipient puts it. Homeland security leaders and practitioners cannot create an adaptive threat orientation with a binge and purge diet of intelligence factoids or just-in-time briefing marathons. Yale philosopher William Graham Sumner (1906, p.632) taught:

> The critical habit of thought, if usual in society, will pervade all its mores, because it is a way of taking up the problems of life. Men educated in it cannot be stampeded by stump orators...They are slow to believe. They

> can hold things as possible or probable in all degrees, without certainty and without pain. They can wait for evidence and weigh evidence, uninfluenced by the emphasis or confidence with which assertions are made on one side or the other. They can resist appeals to their dearest prejudices and all kinds of cajolery.

It is my hope and anticipation that as homeland security leaders, practitioners, politicians, and public awaken to the opportunities for benefit to be gained by prioritizing an adaptive threat orientation that revolutionary improvements to community-wide homeland security decisions may result.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

6 U.S.C. §111(b)(1)(a-h)

6 U.S.C. §48(b)(10)

Abraham, R. (1998, September 7). *Complex dynamical systems*. Lecture notes presented at Neuchatel Summer School, Santa Cruz, CA. Retrieved July 27, 2010 from http://www.ralph-abraham.org/articles/MS%2398.GST2/neu2.fm.pdf

Allpsyche Online. (2007). *Psychology dictionary*. Retrieved July 27, 2010, from http://allpsych.com/dictionary/c.html

Anderson, A. (2005, March 18). *What role for DoD intelligence in support of the homeland security mission.* Carlisle Barracks, PA: U.S. Army War College.

Anikeef, A. H., Bethune, E .R., Gage, L. S., Housman, R. F., Kalberman, S., Krachman, A. B., Manishin, G. B., Martin, E. D., Mathews, L. B., O'Connor, N. M., Savitt, L. J., Sigmund, R. L. & Waldron, J. K. (2003). *Homeland security law handbook: A guide to the legal and regulatory framework*. Rockville MD: Government Institutes.

Bart Everson. (2003). *Elliot Hammer, thinker: A cognitive psychology resource, decision making & heuristics*. Retrieved July 27, 2010, from http://cat.xula.edu/thinker/decisions/heuristics/

Bellavita, C. (2009, March 16). 85% of what you know about homeland security is probably wrong. *Homeland Security Watch*. Retrieved July 27, 2010, from http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/

Borgatti, S. (2009, March 20). *Introduction to grounded theory*. Retrieved from http://www.analytictech.com/mb870/introtoGT.htm

Boyd, J. (2009, March 20). *Organic command and control* Retrieved from http://www.d-n-i.net/boyd/pdf/c&c.pdf

Clarke, S. E. & Chenoweth, E. (2006, January). The politics of vulnerability: Constructing local performance regimes for homeland security. *Review of Policy Research*, *23*(1), 95–114.

Codevilla, A. (2002). *Informing statecraft*. New York: Free Press.

Considine v. City of Waterbury, 279 Conn. 830, 860-69, 905 A.2d 70, 89–95 (Conn. 2006)

Cornell University Law School. (n.d.). *Legal Information Institute. U.S. Constitution (Art. II, Section1).* Retrieved July 27, 2010, from http://topics.law.cornell.edu/constitution/articleii

Cox, J. S. (2004, October 29–30). *The essence of the intelligence function.* Royal Military College of Canada, Canadian Department of National Defense, CDAI-CDFAI 7th Annual Graduate Student Symposium, RMC. Retrieved March 20, 2009, from http://www.cda-cdai.ca/symposia/2004/Cox,%20James-%20Paper.pdf

Cutler, R. (1993, September 22). *Intelligence as a foundation for policy, Central Intelligence Agency Library for the Study of Intelligence*. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no4/pdf/v03i4a05p.pdf, last accessed 20 March 2009

Defense Intelligence Agency. (2008) *Defense intelligence strategy*. Washington, DC: Office of the Under Secretary of Defense for Intelligence.

Demming, D.E. (1999). *Information warfare and security*. New York: ACM Press.

Department of Defense, Defense Intelligence Agency. (2007–2012). *Strategic plan*. Retrieved March 20, 2009, from http://www.dia.mil/thisisdia/2007-2012_DIA_Strategic_Plan_text.htm

Department of Homeland Security. (2004, July 8). *Fact sheet: Homeland Security Operations Center (HSOC)*. [Press release]. Retrieved December 11, 2008, from http://www.dhs.gov/xnews/releases/press_release_0456.shtm

Department of Homeland Security. (2007). *National strategy for homeland security*. Retrieved July 27, 2010, from http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

Department of the Army. (1935). *U.S. Army cavalry manual: Tactics and techniques of cavalry* (6th ed.). Washington DC: author.

Deptula, D. A. (2008). *Lead turning the future: The 2008 strategy for United States Air Force intelligence, surveillance and reconnaissance*. Retrieved March 20, 2009, from http://www.hsdl.org/?view&doc=107794&coll=0

Dulles, A. W. (2006). *The craft of intelligence*. Guillford, CT: Pequot Pres.

Encarta. (n.d.). Retrieved July 27, 2010, from http://encarta.msn.com/encnet/features/dictionary/dictionaryhome.aspx

Federal Bureau of Investigations. *National Security Branch*. Retrieved July 27, 2010, from http://www.fbi.gov/hq/nsb/nsb.htm

Federal Emergency Management Agency. (2009, March 20). *NIMS Resource Center*. Retrieved July 27, 2010, from http://www.fema.gov/emergency/nims/

Findlaw.com. (n.d.). *Reasonable person*. Retrieved July 27, 2010, from http://dictionary.lp.findlaw.com/scripts/results.pl?co=dictionary.lp.findlaw.com&topic=19/194efb4cb63ca323ab32d9ae9418265e

Foster, A. (2005, January). A non-linear model of information seeking behavior. *Information Research, 10*(2). Retrieved July 27, 2010, from http://informationr.net/ir/10-2/paper222.html

Garner, B. A. (1999). *Black's law dictionary* (7th ed.). Eagan, MN: West Group.

Gorman, P. (1992). *Hearings before Select Committee on Intelligence of the United States Senate*. S. 2198 and S. 421. Washington. 262

Harris, J.W. (2002, May 16) Building Leverage in the Long War: Ensuring Intelligence Community Creativity in the Fight Against Terrorism. *Policy Analysis*, pp 3.

Haxton, B. (trans). (2001). *Fragments: The collected wisdom of Heraclitus.* New York: Penguin.

Herman, M. (1999). *Intelligence power in peace, and war*. Cambridge, UK: Cambridge University Press.

Heur, R. J. (1999). *The psychology of intelligence analysis*. Washington, DC: Center for Intelligence Studies, Central Intelligence Agency.

Homeland Security Act. (2002, November 25). *Pub. L. No. 107-296, 116 Stat. 2135.* Retrieved July 27, 2010, from http://dictionary.reference.com/

Hubert, M. & Delor, F. (2000, June). Revisiting the concept of vulnerability. *Social Science and Medicine, 50*(11), 1557–70. Retrieved July 27, 2010, from http://ws5.evision.nl/systeem3/images/WG5%205.%20Revisiting%20the%20concept%20of%20vulnerability.pdf

Institute for Analysis. *Developing and using scenarios for intelligence analysis*. Potomac, MD: author.

Intelligence Reform Act §1011, 50 U.S.C.A. §403-4a(d)(3)

Interagency Threat Assessment and Coordination Group. (2008). *Intelligence guide for first responders*. Washington DC: author. Retrieved July 27, 2010, from http://www.nctc.gov/docs/itacg_guide_for_first_responders.pdf

Jomini, B. A. (1991, spring). The art of war: Clausewitz's contempt for intelligence. *Parameters*.

Justia.com. U.S. Supreme Court Center. (2004). *Executive power: Theory of the presidential office*. Retrieved July 27, 2010, from http://supreme.justia.com/constitution/article-2/02-executive-power.html

Kam, E. (1998). *Surprise attack*. Cambridge, MA: Harvard University Press.

Keegan, J. (2004). *Intelligence in war*. New York: Knopf.

Kellert, S. H. (1993). *In the wake of chaos: Unpredictable order in dynamical systems.* Chicago, IL: University of Chicago Press.

Kent, S. (2009, March 20). Kent's final thoughts on analyst-policy maker relations. *Sherman Kent Center for Intelligence Analysis Occasional Papers, 2*(3). Retrieved March 20, 2009, from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v02n3p.htm

Kessler, G. (2005, May 12). As vote nears: Focus is on Bolton's actions. *Washington Post* (A5).

Klein, G. J. (2003, September-October). Decision navigation: Coping with 21st century challenges in tactical decision making. *Military Review*.

Krawchuk, F. T. (2000, November–December). Developing the capacity for decisive action. *Military Review*, 47–54.

Krizan, L. (1999). *Intelligence essentials for everybody*. Washington DC: Joint Military Intelligence College.

Laquer, W. (1985) *A world of secrets: The uses and limits of intelligence*, New York: Basic Books.

Law.com. *Negligence*. Retrieved March 20, 2009, from http://dictionary.law.com/default2.asp?selected=1314&bold=||||

Lawson, G. (2008, February 7). The fear factory. *Rolling Stone*. Retrieved March 20, 2009, from http://www.rollingstone.com/politics/story/18137343/the_fear_factory

Lee, J. (2003, April 29). E.P.A. said to be concentrating on terror. *New York Times*.

Linder, D. (2010). *U.S. Constitution, 10th Amendment, commentary on separation of powers exploring constitutional conflicts*. Kansas City, MO: City School of Law, University of Missouri-Kansas. Retrieved July 27, 2010, from http://www.law.umkc.edu/faculty/projects/ftrials/conlaw/separationofpowers.htm

Loewenstein, G., O'Donoghue, T. & Rabin, M. (2003, November). Projection bias in predicting future utility. *Quarterly Journal of Economics*, 1210–1248.

Lowenberg, T. (2010). *The role of the National Guard in national defense and homeland security*. Retrieved July 27, 2010, from http://www.ngaus.org/ngaus/files/ccLibraryFiles/Filename/000000000457/primer%20fin.pdf

Magnuson, S. (2010, March). No need to rethink 'no-fly' list criteria, say intelligence chiefs. *National Defense*. Retrieved July 27, 2010, from http://www.nationaldefensemagazine.org/archive/2010/March/Pages/NoNeedtoRethink%E2%80%98No-Fly%E2%80%99List.aspx

Mansdorf, I. J., & Kedar, M. (2008, spring). The psychological asymmetry of Islamist warfare. *Middle East Quarterly*, *15*(2), 37. Retrieved July 27, 2010 from http://www.meforum.org/1867/the-psychological-asymmetry-of-islamist-warfare

Marshall, Chief Justice (1972) *Tatum v. Laird*, 444 F.2d 947, 952-953 (D.C. Cir. 1971). rev'd, 408 U.S. 1

Masse, T. (2006). *Homeland security intelligence: Perceptions, statutory definitions, and approaches*. Washington, DC: Congressional Research Service.

Metzger, G. E. (2003). The Constitutional legitimacy of freestanding federalism. *Harvard Law Review*, 122, 98–107. Retrieved July 27, 2010, from http://www.harvardlawreview.org/media/pdf/LWebsite_Content_for_JenniferForum_Vol._122Metzgermetzger.pdf

Monaghan, H. P. (1970). Presidential war-making. *Boston University Law Review* (special issue), *19*, 25.

Moss, R. (2000, January 29). *Legal effectiveness of a presidential directive as compared to an executive order memorandum for the counsel to the President*. Retrieved July 27, 2010, from http://www.justice.gov/olc/predirective.htm

Neff, J. (2010, March 17) *Comment at AllBusiness.com*. Retrieved July 27, 2010, from http://www.allbusiness.com/marketing-advertising/marketing-advertising/9401966-1.html

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*, 175–220.

Office of the Director of National Intelligence. (2005, October). *National intelligence strategy*. Retrieved March 20, 2009, from http://www.dni.gov/publications/NISOctober2005.pdf

Office of the Director of National Intelligence. Office of General Counsel. (2007, fall) *Intelligence community legal desk reference*. Retrieved from http://biotech.law.lsu.edu/cases/nat-sec/IC_Legal_Reference_Book.pdf

Office of the Director of National Intelligence. *Vision 2015*. Retrieved July 27, 2010, from http://www.dni.gov/Vision_2015.pdf

Office of the President of the United States. (2007, October). *National strategy for homeland security*. Retrieved July 27, 2010, from http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

Onecle. (2005, November 16). *The establishment of judicial review, court opinions*. Retrieved July 27, 2010, from http://law.onecle.com/constitution/article-3/21-judicial-review.html

Pelosi vs. CIA, videotapes for agency, secrecy for Speaker. (2009, July 9). *Wall Street Journal Blog*. Retrieved July 27, 2010, from http://online.wsj.com/article/SB124701436661709153.html

Pfaltzgraff, R. L., Ra'anan, U. & Milberg, W. eds., (1981). American strategic intelligence: politics, priorities and direction. In R. Betts, *Intelligence, policy and national security*. Hamden, CT: Archon Books.

Public Law 107-295. (2002, November 25). Retrieved from July 27, 2010, from http://www.tsa.gov/assets/pdf/MTSA.pdf

Quiggin, T. (2007). *Seeing the invisible: National security intelligence in an uncertain age.* Singapore: World Scientific Publishing Co.

Raghu, T. S., Ramesh, R., & Whinston, A. (2005). Address the homeland security problem: A collaborative decision making framework. *Journal of the American Society for Information Science and Technology*, *56*(3), 312.

Reese, S. (2005). *State and local homeland security: Unresolved issues for the 109th Congress*. Washington DC: Congressional Research Service.

Reyna, V. & Brainerd, C. (2008). Numeracy, ratio bias, and denominator neglect in judgments of risk and probability. *Learning and Individual Differences*, *18*(1) 89–107.

Roy, M.M., Christenfeld, N. J. S., & McKenzie, C. R. M. (2005). The broad applicability of memory bias and its coexistence with the planning fallacy: Reply to Griffin and Buehler. *Psychological Bulletin*, *131*(5), 761–62.

Rumsfeld, D. (2002, February 12). *Department of Defense*. [Press briefing]. http://www.iii.org/media/hottopics/insurance/terrorism/ Retrieved July 27, 2010, from http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

Saha A. N. (1990). *Mitra's legal & commercial dictionary* (4th ed). New Delhi: Eastern Law House.

Senator Richard Shelby, *September 11 and the imperative of reform in the U.S. Intelligence Community*. (2002, December 10). Retrieved from http://intelligence.senate.gov/shelby.pdf last accessed 27 JUL 10

Shambach, S.A. (1996, October 1-2) *Strategic decision-making in the information age.* Report on the Strategic Leadership Workshop, Army War College, Carlisle Barracks, PA. Retrieved July 27, 2010, from http://www.au.af.mil/au/awc/awcgate/stratdm.htm

Sims, J.E. & Gerber, B. (2005). *Transforming U.S. intelligence.* Washington DC: Georgetown University Press.

Snider, L. B. (1997, February). *Sharing Secrets with lawmakers: An intelligence monograph*. Retrieved July 27, 2010, from http://www.globalsecurity.org/intell/library/reports/1997/sharing-secrets-congress.htm

Spadanuta, L. (2008, January). An intelligence sharing success story. *Security Management*.

Stafford, R. T. Disaster Relief and Emergency Assistance Act, (P.L. 93-288, as amended, 42 U.S.C. §§ 5121-5206)

Steele-Vivas, R.D. (2002 May 15). Creating a smart nation: Strategy, policy, intelligence, and information. *Government Information Quarterly*, *13*(2)159–173

Stephen Dycus, Arthur L. Berney, William C. Banks, & Peter Raven-Hanse. (2002). National Security Law (3rd ed.). New York: Aspen Publishers.

Sulistyawati, K. & Chui, Y.P. (2009). *Confidence Bias in Situational Awareness, Lecture Notes on Artificial Intelligence*; *Vol 5639*. Proceedings of the 8th International Conference on Engineering Psychology and Cognitive Ergonomics, San Diego, CA. Retrieved from July 27, 2010, from http://www.springerlink.com/content/w7x2n7kv41330740/

Sullivan, R. (2010, July 7). Head on collision of interests. *Financial Times.* Retrieved from October 13, 2009, from *http://blogs.ft.com/ftfmblog/2009/10/13/head-on-collision-of-interests/*

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable.* New York: Random House.

Terrorism risk and insurance. (2002, November 26). Retrieved July 27, 2010, from http://www.iii.org/media/hottopics/insurance/terrorism/

Tenet, G. (1995, June 14). Prepared Statement at DDCI Confirmation Hearing Before the Senate Select Committee on Intelligence. Retrieved July 27, 2010, from https://www.cia.gov/news-information/speeches-testimony/1995/ddci_speech_61495.html

Tetlock, P.E. & Levi, A. (1982). Attribution Bias: On the inconclusiveness of the cognition—Motivation debate. *Journal of Experimental Social Psychology, 18*, 68–88.

Treverton G. F. (2001 November 1). *National security intelligence crisis*. Retrieved July 27, 2010, from http://www.govexec.com/features/1101/1101s1.htm

Treverton, G. F. (2009). *Intelligence in an age of terror.* Cambridge: Cambridge University Press.

Treverton, G. (2001). *Reshaping national intelligence for an age of information*. Cambridge: Cambridge University Press.

Treverton, G.F. & Gabbard, C.B. (2008). *Assessing the tradecraft of intelligence analysis*. Arlington VA: RAND.

Turner, M. (2005). *Why secret intelligence fails.* Washington D.C.: Potomac.

Tzu, S. translated by Minford, J. (2002). *The art of war*. New York: Viking.

U.S. Supreme Court Center. *Police powers*. Retrieved from March 20, 2009, from http://supreme.justia.com/constitution/amendment-14/79-police-power-regulation.html

United States Constitution Art II, § 8

United States Department of Justice, Office of the Attorney General, Retrieved March 20, 2009, from http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf

Viana, L. P. *HS Today news and analysis—Spies and the city*. Retrieved December 8, 2008, from http://hstoday.us./content/view/4924/27/

Wheaton, K. (2010, April 17). *Comment on defining intelligence* (Intelligence Professionals LinkedIn Discussion Board). Retrieved July 27, 2010, from http://www.linkedin.com/groups?mostPopular=&gid=72244&goback=%2Egna_72244

White House. (n.d.). *Homeland Security.* Retrieved August 11, 2010, from http://www.whitehouse.gov/issues/homeland-security

White House, (1982, April 10) *National security decision directive 30,* Retrieved March 20, 2009, from http://www.fas.org/irp/offdocs/nsdd/nsdd-030.htm

White House. (2003). *Homeland security presidential directive 5: Management of domestic incidents.* Retrieved July 27, 2010, from http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision.* Stanford, CA: Stanford University Press.

Wolgast, K. (2005). *Command Decision making: experience counts*. Master's thesis. U.S. Army War College, Carlisle, PA.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California